КОМИТЕТ ПО ДЕЛАМ ОБРАЗОВАНИЯ ГОРОДА ЧЕЛЯБИНСКА
МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ
«ДВОРЕЦ ПИОНЕРОВ И ШКОЛЬНИКОВ ИМ. Н.К. КРУПСКОЙ Г.ЧЕЛЯБИНСКА»

ПРИКАЗ

«19» 01 2026 г. № 22-09

Об организации работ по обработке и обеспечению безопасности персональных данных

С целью организации работ по обеспечению безопасности персональных данных при ее обработке в информационных системах МАУДО «ДПШ» в соответствии с требованиями Федерального Закона РФ от 27.07.2006 № 152-ФЗ «О персональных данных», постановления Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказа ФСТЭК РФ №21 от 18.02.2013 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие:
   1) политику обработки и защиты персональных данных МАУДО «ДПШ» (Приложение 1);
   2) политику конфиденциальности МАУДО «ДПШ» (Приложение 2);
   3) пользовательское соглашение МАУДО «ДПШ» (Приложение 3);
   4) перечень персональных данных, обрабатываемых МАУДО «ДПШ» (Приложение 4);
   5) положение об обработке персональных данных с использованием средств автоматизации (Приложение 5);
   6) положение об обработке персональных данных без использования средств автоматизации (Приложение 6);
   7) правила обработки персональных данных (Приложение 7);
   8) правила рассмотрения запросов субъектов персональных данных или Уполномоченного органа по защите прав субъектов персональных данных (Приложение 8);
   9) правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (Приложение 9);

10) инструкцию по резервному копированию и восстановления персональных данных (Приложение 10);

11) инструкцию по антивирусной защите информационной системы МАУДО «ДПШ» (Приложение 11);

12) инструкцию по использованию корпоративной сети передачи персональных данных (Приложение 12);

13) инструкция по организации парольной защиты (Приложение 13);

14) инструкцию ответственного за организацию обработки персональных данных (Приложение 14);

15) инструкцию ответственного за обеспечение безопасности персональных данных в информационной системе (Приложение 15);

16) форму журнала учёта обращений субъектов персональных данных (Приложение 16);

17) форму журнала учёта работ в информационной системе МАУДО «ДПШ» (Приложение 17);

18) форму журнала учёта съёмных носителей информации (Приложение 18);

19) форму журнала учёта ключей от сейфов и помещений (Приложение 19);

20) форму акта уничтожения персональных данных на электронных носителях (Приложение 20);

21) форму акта уничтожения носителей персональных данных (Приложение 21);

22) форму соглашения о неразглашении информации (Приложение 22);

23) форму согласия на обработку персональных данных различных категорий субъектов персональных данных (Приложение 23);

24) перечень мест хранения материальных носителей персональных данных (Приложение 24);

25) перечень информационных систем МАУДО «ДПШ» (Приложение 25);

26) перечень должностей работников МАУДО «ДПШ», доступ которых к защищаемой информации необходим для выполнения ими должностных обязанностей (Приложение 26);

2. Назначить ответственным за организацию обработки персональных данных в МАУДО «ДПШ» Завьялова А.А., первого заместителя директора, с возложением на него обязанностей в соответствии с инструкцией ответственного за организацию обработки персональных данных.

3. Назначить ответственным за обеспечение безопасности персональных данных в информационной системе МАУДО «ДПШ» Гладкова К.Н., программиста МАУДО «ДПШ», с возложением на него обязанностей в соответствии с инструкцией ответственного за обеспечение безопасности персональных данных в информационной системе.

4. Определить границей контролируемой зоны МАУДО «ДПШ» (далее – контролируемая зона) ограждающие конструкции зданий, располагающихся по

адресу: 454080, Россия, Челябинская область, г. Челябинск, Свердловский пр., 59; 454021, г. Челябинск, пр. Героя России Евгения Родионова, 13:

27) разрешить пребывание посторонних лиц на территории контролируемой зоны только в присутствии и под контролем работников, допущенных к работе в информационных системах МАУДО «ДПШ»;

28) все помещения контролируемой зоны в нерабочее время подлежат закрытию на ключ и сдаче под охрану;

29) возложить ответственность за обеспечение безопасности в защищаемых помещениях на Павлухина Д.В. заместителя директора по обеспечению комплексной безопасности

5. Создать комиссию по вопросам обработки персональных данных в МАУДО «ДПШ» (Приложение 27).

6. Комиссии по вопросам обработки персональных данных:

- определить уровни защищенности персональных данных выявленных информационных систем персональных данных;

- оценить возможный вред субъектам, чьи персональные данные обрабатываются в информационных системах персональных данных.

7. Комиссии по вопросам обработки персональных данных производить уничтожение носителей информации по мере необходимости. Факт уничтожения носителей информации фиксируется в акте уничтожения носителя персональных данных субъекта (ов) (Приложения 20 и 21).

8. Утвердить План внутренних проверок защищенности персональных данных (приложение 28).

9. Ответственному за организацию обработки персональных данных Завьялову А.А. и ответственному за обеспечение безопасности персональных данных в информационной системе Гладкову К.Н. провести работы по обеспечению безопасности информации в соответствии с прилагаемым Планом внутренних проверок защищенности персональных данных.

Директор Ю.В. Смирнова

Завьялов А.А.
220 08 51
Разослать: в дело, исполнителю, бухгалтерию, заместителям директора, структурные подразделения, филиал

Приложение 1
к приказу МАУДО «ДПШ»
от 19.01.26 № 22-од

Политика
обработки и защиты персональных данных

I. Общие положения

1. В целях соблюдения законодательства Российской Федерации, регулирующего отношения, связанные с обработкой и обеспечением безопасности персональных данных, а также поддержания деловой репутации Муниципального автономного учреждения дополнительного образования «Дворец пионеров и школьников им. Н.К. Крупской г. Челябинска» (далее – МАУДО «ДПШ») считает своими задачами соблюдение принципов законности, справедливости и конфиденциальности при обработке персональных данных, а также обеспечение безопасности процессов их обработки.

2. Настоящая Политика в отношении обработки и защиты персональных данных в МАУДО «ДПШ» (далее – Политика):

1) раскрывает основные категории персональных данных, обрабатываемых МАУДО «ДПШ», цели, способы и принципы обработки персональных данных, права и обязанности МАУДО «ДПШ» при обработке персональных данных, права субъектов персональных данных;

2) является общедоступным документом, декларирующим концептуальные основы деятельности МАУДО «ДПШ» при обработке персональных данных.

3. Термины и определения, используемые в Политике:

Биометрические персональные данные - сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных.

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Доступ к информации (доступ) - ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации.

Информационная система персональных данных (далее – ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Несанкционированный доступ (НСД) – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т.

различных организаций путём изменения (повышения, фальсификации) своих прав доступа.

Носитель информации – любой материальный объект или среда, используемый для хранения или передачи информации.

Персональные данные (далее – ПДн) - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными. Оператором является МАУДО «ДПШ».

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Специальные категории персональных данных - категории персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

Субъект персональных данных (субъект) — физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных.

Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

4. Основные права субъектов персональных данных:

1) субъект персональных данных имеет право на получение сведений об обработке его персональных данных в МАУДО «ДПШ»;

2) субъект персональных данных вправе требовать от МАУДО «ДПШ», который их обрабатывает, уточнения этих персональных данных, их блокирования или уничтожения в случае, если они являются неполными, устаревшими, неточными, незаконно полученными или не могут быть признаны необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

3) право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами;

4) для реализации своих прав и защиты законных интересов субъект персональных данных имеет право обратиться к МАУДО «ДПШ». Оператор рассматривает любые обращения и жалобы со стороны субъектов персональных данных, тщательно расследует факты нарушений и принимает все необходимые меры для их немедленного устранения, наказания виновных лиц и урегулирования спорных и конфликтных ситуаций в досудебном порядке;

5) субъект персональных данных вправе обжаловать действия или бездействие МАУДО «ДПШ» путем обращения в Уполномоченный орган по защите прав субъектов персональных данных (территориальный орган Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций);

6) субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и/или компенсацию морального вреда в судебном порядке.

5. Основные обязанности МАУДО «ДПШ»:

1) соблюдать требования законодательства РФ в области обработки и защиты персональных данных;

2) при сборе персональных данных предоставить субъекту персональных данных по его просьбе информацию, касающуюся обработки персональных данных;

3) если предоставление персональных данных является обязательным в соответствии с федеральным законом, работники МАУДО «ДПШ» обязаны разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные;

4) при сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации;

5) опубликовать или иным образом обеспечить неограниченный доступ к актуальному документу, определяющему его политику в отношении обработки

персональных данных, к сведениям о реализуемых требованиях к защите персональных данных (настоящую Политику);

6) принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним;

7) сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя;

8) уточнять персональные данные Субъектов, блокировать или уничтожать их в случае, если они являются неполными, устаревшими, неточными, незаконно полученными или не могут быть признаны необходимыми для заявленной цели обработки;

9) прекратить обработку персональных данных в случае отзыва субъектом персональных данных согласия на обработку его персональных данных. МАУДО «ДПШ» вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных».

II. Цели сбора персональных данных

6. МАУДО «ДПШ» обрабатывает следующие категории субъектов персональных данных (далее – Субъекты):

1) работники МАУДО «ДПШ», бывшие работники, соискатели для приема на работу, а также ближайшие родственники работников;

2) педагоги – члены рабочих групп, экспертных советов, оргкомитета, жюри;

3) обучающиеся и их родители (законные представители);

4) персональные данные физических лиц, состоящих в гражданско-правовых отношениях.

7. МАУДО «ДПШ» обрабатывает персональные данные работников исключительно в следующих целях:

1) выполнение требований законодательства Российской Федерации;

2) осуществление трудовых отношений;

3) ведение бухгалтерского, налогового и кадрового учета;

4) совершенствование профессиональных знаний и продвижение по службе;

5) обеспечение личной безопасности;

6) перечисление денежных средств в банк;

7) информирование граждан;

8) постоянная связь с поставщиком услуг;

9) контроль за исполнением условий контракта.

8. МАУДО «ДПШ» обрабатывает персональные данные ближайших родственников работников исключительно в целях ведения кадрового делопроизводства.

9. МАУДО «ДПШ» обрабатывает персональные данные бывших работников исключительно в следующих целях:

1) ведения бухгалтерского, налогового учета;

2) информирования граждан.

10. МАУДО «ДПШ» обрабатывает персональные данные соискателей исключительно в целях принятия решения о трудоустройстве соискателя в МАУДО «ДПШ».

11. МАУДО «ДПШ» обрабатывает персональные данные педагогов – членов рабочих групп исключительно в целях участия в составе рабочей группы конкурса.

12. МАУДО «ДПШ» обрабатывает персональные данные педагогов – членов экспертных советов исключительно в целях участия в составе экспертного совета.

13. МАУДО «ДПШ» обрабатывает персональные данные педагогов – членов оргкомитета-жюри исключительно в целях участия в составе оргкомитета-жюри.

14. МАУДО «ДПШ» обрабатывает персональные данные обучающихся исключительно в следующих целях:

1) предоставления образовательных услуг;

2) участия обучающихся в конкурсах, олимпиадах и других мероприятиях;

3) осуществления психолого-педагогического сопровождения;

4) составления отчетности о работе МАУДО «ДПШ»;

5) информирования граждан.

15. МАУДО «ДПШ» обрабатывает персональные данные родителей (законных представителей) обучающихся исключительно в следующих целях:

1) предоставления образовательных услуг;

2) осуществления психолого-педагогического сопровождения;

3) составления отчетности о работе МАУДО «ДПШ».

16. МАУДО «ДПШ» обрабатывает персональные данные физических лиц и индивидуальных предпринимателей, состоящих в гражданско-правовых отношениях, исключительно в целях заключения и выполнения обязательств по договорам.

III. Правовые основания обработки персональных данных

17. Правовым основанием обработки персональных данных является совокупность правовых актов, во исполнение которых и в соответствии с которыми МАУДО «ДПШ» осуществляет обработку персональных данных.

18. Обработка персональных данных в МАУДО «ДПШ» осуществляется в соответствии со следующими правовыми основаниями:

1) Конституция Российской Федерации от 25.12.1993;

2) Трудовой кодекс Российской Федерации от 30.12.2001 №197-ФЗ;

3) Гражданский кодекс Российской Федерации от 30.11.1994 №51-ФЗ;

4) Уголовный кодекс Российской Федерации от 13.06.1996 №63-ФЗ;

5) Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 №195-ФЗ;

6) Налоговый Кодекс Российской Федерации часть первая от 31.07.1998 №146-ФЗ и часть вторая от 05.08.2000 №117-ФЗ (с изменениями и дополнениями);

7) Федеральный закон от 19.12.2005 №160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;

8) Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;

9) Федеральный закон от 01.04.1996 №27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»;

10) Федеральный закон от 28.03.1998 №53-ФЗ «О воинской обязанности и военной службе»;

11) Федеральный закон от 02.05.2006 №59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;

12) Федеральный закон РФ от 15.12.2001 №167-ФЗ «Об обязательном пенсионном страховании»;

13) Закон РФ от 07.02.1992 №2300-1 «О защите прав потребителей»;

14) Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных»;

15) Постановление Правительства РФ от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

16) Постановление Правительства РФ от 17.12.2013 №1177 «Об утверждении Правил организованной перевозки группы детей автобусами»;

17) Постановление Правительства Российской Федерации от 10.07.2013 №582 «Об утверждении правил размещения на официальном сайте образовательной организации в информационно-телекоммуникационной сети «Интернет» и обновления информации об образовательной организации»;

18) Постановление Правительства Российской Федерации от 15.08.2013 №706 «Об утверждении Правил оказания платных образовательных услуг»;

19) Постановление правления пенсионного фонда Российской Федерации от 31.07.2006 №192п «О формах документов индивидуального (персонифицированного)

учета в системе обязательного пенсионного страхования и инструкции по их заполнению»;

20) Федеральный закон от 02.05.2006 №59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;

21) Федеральный закон от 29.11.2010 №326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»;

22) Приказ МВД России от 30.12.2016 №941 «Об утверждении Порядка подачи уведомления об организованной перевозке группы детей автобусами»;

23) Приказ Минкультуры России от 25.08.2010 №558 «Об утверждении «Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения»;

24) Приказ Минобрнауки России от 25.10.2013 №1185 «Об утверждении примерной формы договора об образовании на обучение по дополнительным образовательным программам»;

25) Устав МАУДО «ДПШ»;

26) коллективный договор;

27) трудовые договоры с работниками;

28) договоры, заключаемые между МАУДО «ДПШ» и субъектом персональных данных;

29) согласия субъектов на обработку персональных данных.

IV. Объем и категории обрабатываемых персональных данных, категории субъектов персональных данных

19. Содержание и объем обрабатываемых персональных данных субъектов соответствует целям обработки.

20. В рамках обработки персональных данных работников обрабатываются следующие категории персональных данных:

1) фамилия, имя, отчество;

2) ИНН;

3) СНИЛС (№ страхового пенсионного свидетельства);

4) табельный номер;

5) пол;

6) номер, дата трудового договора;

7) дата рождения;

8) место рождения;

9) гражданство;

10) образование (среднее (полное) общее, начальное профессиональное, среднее профессиональное, высшее профессиональное, аспирантура, адъюнктура, докторантура);

11) наименование образовательного учреждения;

12) наименование, серия, номер, дата выдачи, направление или специальность, код по ОКСО, ОКИН документа об образовании, о квалификации или наличии специальных знаний;

13) профессия (в т.ч. код по ОКПДТР);

14) стаж работы;

15) состояние в браке;

16) состав семьи, с указанием степени родства, фамилии, имени, отчества, года рождения ближайших родственников;

17) данные документа, удостоверяющего личность (вид, серия, номер, дата выдачи, наименование органа, выдавшего документ);

18) адрес и дата регистрации;

19) фактический адрес места жительства;

20) телефон;

21) сведения об отношении к воинской службе;

22) дата приема на работу;

23) характер работы;

24) вид работы (основной, по совместительству);

25) структурное подразделение;

26) занимаемая должность (специальность, профессия), разряд, класс (категория) квалификации;

27) ранее занимаемая должность;

28) тарифная ставка (оклад), надбавка, руб.;

29) основание трудоустройства;

30) личная подпись работника;

31) электронная подпись;

32) сведения об аттестации (дата, решение, номер и дата документа, основание);

33) сведения о профессиональной подготовке (дата начала и окончания переподготовки, специальность (направление, профессия, наименование, номер, дата документа, свидетельствующего о переподготовке, основание переподготовки);

34) сведения о наградах, поощрениях, почетных званиях (наименование, номер, дата награды);

35) сведения об отпусках (вид, период работы, количество дней, дата начала и окончания, основание);

36) сведения о социальных льготах, на которые работник имеет право в соответствии с законодательством (наименование льготы, номер, дата выдачи документа, основание);

37) сведения об увольнении (основания, дата, номер и дата приказа);

38) объем работы;

39) сведения о доходах;

40) сведения из трудовой книжки;

41) сведения из личной медицинской книжки;

42) сведения из водительского удостоверения;

43) место работы;

44) адрес электронной почты;

45) номер банковской карты;

46) номер лицевого счета;

47) фотография.

21. В рамках обработки персональных данных ближайших родственников работников обрабатываются следующие категории персональных данных:

1) фамилия, имя, отчество;

2) степень родства;

3) год рождения.

22. В рамках обработки персональных данных бывших работников обрабатываются следующие категории персональных данных:

1) фамилия, имя, отчество;

2) ИНН;

3) СНИЛС (№ страхового пенсионного свидетельства);

4) номер, дата трудового договора;

5) дата рождения;

6) место рождения;

7) данные документа, удостоверяющего личность (вид, серия, номер, дата выдачи, наименование органа, выдавшего документ);

8) дата приема на работу;

9) характер работы;

10) вид работы (основной, по совместительству);

11) структурное подразделение;

12) занимаемая должность (специальность, профессия), разряд, класс (категория) квалификации;

13) тарифная ставка (оклад), надбавка, руб.;

14) основание трудоустройства;

15) сведения об отпусках (вид, период работы, количество дней, дата начала и окончания, основание);

16) сведения о социальных льготах, на которые работник имеет право в соответствии с законодательством (наименование льготы, номер, дата выдачи документа, основание);

17) сведения об увольнении (основания, дата, номер и дата приказа);

18) объем работы;

19) сведения о доходах;

20) номер банковской карты;

21) номер лицевого счета;

22) фотография.

23. В рамках обработки персональных данных соискателей обрабатываются следующие категории персональных данных:

1) фамилия, имя, отчество;

2) образование;

3) специальность;

4) профессия;

5) предыдущий опыт работы;

6) стаж по специальности;

7) контактный телефон;

8) адрес электронной почты.

24. В рамках обработки персональных данных педагогов – членов рабочих групп, экспертных советов, оргкомитета, жюри обрабатываются следующие категории персональных данных:

1) фамилия, имя, отчество;

2) наименование учреждения;

3) должность;

4) контактный телефон.

25. В рамках обработки персональных данных обучающихся обрабатываются следующие категории персональных данных:

1) фамилия, имя, отчество;

2) дата рождения;

3) место рождения;

4) пол;

5) класс;

6) сведения о посещаемости занятий;

7) контактный телефон;

8) электронная почта;

9) данные о состоянии здоровья;

10) данные об инвалидности;

11) фотография;

12) данные документа, удостоверяющего личность (вид, серия, номер, дата выдачи, наименование органа, выдавшего документ);

13) ИНН;

14) СНИЛС (№ страхового пенсионного свидетельства);

15) автобиография;

16) домашний адрес;

17) домашний телефон;

18) страница в социальной сети;

19) наличие знания языков;

20) хобби;

21) наименование образовательной организации;

22) наименование секции;

23) сведения о полученных наградах и достижениях;

24) сведения о родителях (законных представителях).

26. В рамках обработки персональных данных родителей (законных представителей) воспитанников обрабатываются следующие категории персональных данных:

1) фамилия, имя, отчество;

2) данные документа, удостоверяющего личность (вид, серия, номер, дата выдачи, наименование органа, выдавшего документ);

3) домашний адрес;

4) место работы;

5) должность;

6) контактный телефон;

7) личная подпись.

27. В рамках обработки персональных данных физических лиц, состоящих в гражданско-правовых отношениях, обрабатываются следующие категории персональных данных:

1) фамилия, имя, отчество;

2) адрес регистрации ИП;

3) домашний адрес;

4) ИНН;

5) ОГРН;

6) номер расчетного счета;

7) название банка;

8) контактный телефон.

28. МАУДО «ДПШ» не осуществляет обработку биометрических персональных данных (сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются для установления личности субъекта персональных данных).

29. МАУДО «ДПШ» не осуществляет обработку специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

V. Порядок и условия обработки персональных данных

30. В МАУДО «ДПШ» обработка персональных данных субъектов осуществляется в целях, указанных в разделе II настоящей Политики.

31. В МАУДО «ДПШ» обрабатываются категории персональных данных, указанные в разделе IV настоящей Политики.

32. Обработка персональных данных в МАУДО «ДПШ» осуществляется в соответствии с законодательством Российской Федерации в рамках полномочий и при условии получения согласия субъектов персональных данных. Согласие субъекта персональных данных оформляется в письменной форме, если иное не установлено Федеральным законом №152-ФЗ от 27.07.2006 «О персональных данных».

33. Обработка персональных данных субъектов включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

34. Обработка фотографий работников и иных субъектов осуществляется только при условии получения согласия субъектов персональных данных. Обработка осуществляется с использованием средств автоматизации.

35. МАУДО «ДПШ» не осуществляет трансграничную (на территории иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу) передачу персональных данных.

36. В МАУДО «ДПШ» созданы общедоступные источники персональных данных (сайт, информационный стенд). Персональные данные (фамилия, имя, отчество, должность, квалификация, год рождения, и др.), сообщаемые субъектом (работником/гражданином), включаются в такие источники в соответствии с законодательством Российской Федерации в рамках полномочий и с письменного согласия субъекта персональных данных.

37. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляется путем получения персональных данных непосредственно от субъектов персональных данных (их законных представителей).

38. МАУДО «ДПШ» и работники МАУДО «ДПШ», получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

39. МАУДО «ДПШ» вправе передавать персональные данные органам дознания и следствия, иным уполномоченным органам по основаниям, предусмотренным действующим законодательством Российской Федерации.

40. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, работник МАУДО «ДПШ», осуществляющий

сбор (получение) персональных данных непосредственно от субъектов персональных данных, обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

41. МАУДО «ДПШ» в своей деятельности обеспечивает соблюдение принципов обработки персональных данных, указанных в ст.5 Федерального закона №152-ФЗ «О персональных данных».

42. МАУДО «ДПШ» в своей деятельности принимает меры, предусмотренные ч.2 ст.18.1, ч.1 ст.19 Федерального закона №152-ФЗ «О персональных данных».

43. В МАУДО «ДПШ» не используются для обработки персональных данных базы данных, находящиеся за пределами границ Российской Федерации.

44. Условия прекращения обработки персональных данных МАУДО «ДПШ»:

1) достижение целей обработки персональных данных;

2) истечение срока действия согласия или отзыв согласия субъекта персональных данных на обработку его персональных данных;

3) выявление неправомерной обработки персональных данных.

45. Назначенными лицами МАУДО «ДПШ» осуществляется контроль за хранением и использованием материальных носителей персональных данных, не допускающий несанкционированное использование, уточнение, распространение и уничтожение персональных данных, находящихся на этих носителях.

46. Срок хранения персональных данных в форме, позволяющей определить субъекта персональных данных, осуществляется не дольше, чем этого требуют цели обработки персональных данных, кроме случаев, когда срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

47. В целях соблюдения законодательства РФ, для достижения целей обработки, а также в интересах и с согласия субъектов персональных данных МАУДО «ДПШ» в ходе своей деятельности предоставляет персональные данные следующим организациям:

1) Федеральной налоговой службе;

2) Пенсионному фонду России;

3) Страховым компаниям;

4) Комитету по делам образования города Челябинска;

5) Образовательным учреждениям;

6) ПАО «Росбанк»;

7) ООО «Образовательная практика»;

8) ООО Туристская компания «Одиссея»;

9) ЧУ ДО ПАО «ММК» «Детский оздоровительно-образовательный комплекс»;

10) МАУ ДОЛ «Солнечная поляна»;

11) Иным третьим лицам в соответствии с заключенными договорами.

VI. Актуализация, исправление, удаление и уничтожение персональных данных, ответы на запросы субъектов на доступ к персональным данным

48. В случае выявления неправомерной обработки персональных данных МАУДО «ДПШ» осуществляет блокирование неправомерно обрабатываемых персональных данных.

49. В случае выявления неточных персональных данных МАУДО «ДПШ» осуществляет блокирование соответствующих персональных данных на период проверки. В случае подтверждения факта неточности персональных данных МАУДО «ДПШ» на основании сведений, представленных субъектом персональных данных или его представителем либо Уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов уточняет персональные данные и снимает блокирование персональных данных.

50. МАУДО «ДПШ» обязан сообщить субъекту персональных данных или его представителю информацию об осуществляемой им обработке персональных данных такого субъекта по запросу последнего.

51. Сведения, касающиеся обработки персональных данных, предоставляются субъекту персональных данных или его представителю при получении запроса субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

52. Рассмотрение запросов субъектов персональных данных или их представителей, а также Уполномоченного органа по защите прав субъектов персональных данных:

1) субъекты персональных данных имеют право на получение информации, касающейся обработки их персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных в МАУДО «ДПШ»;
- правовые основания и цели обработки персональных данных;
- применяемые в МАУДО «ДПШ» способы обработки персональных данных;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения в МАУДО «ДПШ»;
- порядок осуществления субъектом персональных данных прав, предусмотренных законодательством Российской Федерации в области персональных данных;

- иные сведения, предусмотренные законодательством Российской Федерации в области персональных данных.

2) при получении запроса субъекта персональных данных или его представителя, а также Уполномоченного органа по защите прав субъектов персональных данных, МАУДО «ДПШ» предоставляет сведения в сроки в соответствии требований статьи 20 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных».

53. Субъекты персональных данных вправе требовать от МАУДО «ДПШ» уточнения их персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав

54. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе, если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

55. Для получения необходимой информации, касающейся обработки персональных данных, описанной в п.п.52 и 53 настоящей Политики, субъекту (либо законному представителю) необходимо заполнить соответствующую форму запроса субъекта персональных данных информации, касающейся обработки персональных данных и передать лично работникам МАУДО «ДПШ», принимающим обращения граждан, либо по почте. Формы запросов субъекта персональных данных представлены в Правилах рассмотрения запросов субъектов персональных данных или Уполномоченного органа по защите прав субъектов персональных данных.

56. При достижении целей обработки персональных данных, а также в случае отзыва субъектом персональных данных согласия на их обработку персональные данные подлежат уничтожению, если:

1) иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;

2) иное не предусмотрено иным соглашением между МАУДО «ДПШ» и субъектом персональных данных.

57. При получении запроса субъекта персональных данных или его представителя, а также Уполномоченного органа по защите прав субъектов персональных данных, по устранению нарушений законодательства, допущенных при обработке персональных данных, по уточнению, блокированию и уничтожению персональных данных, МАУДО «ДПШ» осуществляет соответствующие меры и уведомляет о выполненных мерах в сроки согласно требованиям статьи 21 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных».

VII. Обеспечение защиты персональных данных при их обработке

58. МАУДО «ДПШ» предпринимает необходимые правовые, организационные и технические меры для обеспечения защиты персональных данных от случайного или преднамеренного доступа, уничтожения, изменения, блокирования и других несанкционированных действий.

59. Предпринимаются следующие меры, направленные на обеспечение безопасности обработки персональных данных субъектов:

1) назначение ответственного лица за организацию обработки персональных данных;

2) принятие документов, определяющих политику организации в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

3) осуществление внутреннего контроля соответствия обработки персональных данных Российскому законодательству и требованиям регулирующих органов;

4) ознакомление работников организации, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику организации в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных;

5) проводится оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения «Закона о персональных данных», определяется соотношение указанного вреда и принимаемых МАУДО «ДПШ» мер, направленных на обеспечение исполнения обязанностей, предусмотренных «Законом о персональных данных».

60. Обеспечение защиты персональных данных в МАУДО «ДПШ» при их обработке, осуществляемой без использования средств автоматизации, достигается, в частности, путем:

1) обособления персональных данных от иной информации;

2) недопущения фиксации на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы;

3) использования отдельных материальных носителей для обработки каждой категории персональных данных;

4) принятия мер по обеспечению раздельной обработки персональных данных при несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не

позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных;

5) использования типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных;

6) обеспечения раздельного хранения персональных данных (материальных носителей), обработка которых осуществляется в различных целях, и установлению перечня лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

Требования к мерам защиты персональных данных и способы реализации этих требований осуществляются в соответствии с руководящими и методическими документами ФСТЭК России и ФСБ России.

61. Обеспечение безопасности персональных данных осуществляется путем выполнения комплекса правовых, организационных и технических мероприятий, реализуемых в рамках создаваемой системы защиты персональных данных (СЗПДн).

62. Защита персональных данных осуществляется для исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

63. Методами и способами защиты информации от несанкционированного доступа в создаваемой автоматизированной СЗПДн являются:

1) реализация разрешительной системы допуска сотрудников (обслуживающего персонала) к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам;

2) ограничение доступа сотрудников в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации;

3) разграничение доступа сотрудников к информационным ресурсам, программным средствам обработки (передачи) и защиты информации; доступ Работников к обрабатываемым персональным данным осуществляется в соответствии с их должностными обязанностями и требованиями внутренних документов МАУДО «ДПШ»;

4) регистрация действий сотрудников, контроль несанкционированного доступа и действий сотрудников и посторонних лиц;

5) учет и хранение съемных носителей информации и их обращение, исключающее хищение, подмену и уничтожение;

6) использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;

7) использование защищенных каналов связи;

8) размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах охраняемой территории;

9) организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку персональных данных;

10) предотвращение внедрения в информационные системы вредоносных программ.

VIII. Заключительные положения

64. Настоящая политика является внутренним документом МАУДО «ДПШ», общедоступной и подлежит размещению на официальном сайте МАУДО «ДПШ».

65. Настоящая политика подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных, но не реже одного раза в три года.

66. Контроль исполнения требований настоящей Политики осуществляется ответственным за организацию обработки персональных данных в МАУДО «ДПШ».

67. Ответственность должностных лиц МАУДО «ДПШ», имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных, определяется в соответствии с законодательством Российской Федерации и внутренними документами МАУДО «ДПШ».

Приложение 2
к приказу МАУДО «ДПШ»
от 19.01.26 № 22-09

Политика конфиденциальности МАУДО «ДПШ»

I. Общие положения

1. Политика конфиденциальности персональной информации (далее – Политика) действует в отношении всей информации, которую МАУДО «ДПШ» может получить о пользователе сети Интернет (далее – Пользователь) во время использования им сайта www.chel-dpsh.ru (далее – Сайт) в ходе исполнения МАУДО «ДПШ» любых соглашений и договоров с Пользователем.

2. Использование Сайта означает безоговорочное согласие Пользователя с настоящей Политикой и указанными в ней условиями обработки его персональной информации. В случае несогласия с этими условиями Пользователь должен воздержаться от использования Сайта.

II. Персональная информация Пользователя, которую обрабатывает МАУДО «ДПШ»

3. В рамках настоящей Политики под персональной информацией Пользователя понимается:

- персональная информация, осознанно предоставленная Пользователем во время процедуры заполнения и отправки форм Сайта (оставить комментарий), такая как имя, электронный адрес;
- данные для авторизации в личном кабинете, осознанно предоставленные Пользователем для авторизации на Сайте;
- техническая информация, автоматически собираемая программным обеспечением Сайта во время его посещения.

4. Во время посещения Сайта, администрации Сайта автоматически становится доступной информация из стандартных журналов регистрации сервера (server logs). Сюда включается IP-адрес компьютера (или прокси-сервера, если он используется для выхода в Интернет), имя Интернет-провайдера, имя домена, тип браузера и операционной системы, информация о сайте, с которого Пользователь совершил переход на Сайт, страницах Сайта, которые Пользователь посещает, дате и времени этих посещений, файлах, которые Пользователь загружает. Эта информация анализируется в агрегированном (обезличенном) виде для анализа посещаемости Сайта, и используется при разработке предложений по его улучшению и развитию.

5. Связь между IP-адресом Пользователя и его персональной информацией никогда не раскрывается третьим лицам, за исключением тех случаев, когда этого требует законодательство.

6. Информация о посещении Сайта фиксируется установленными статистическими счетчиками Сайта.

III. Цели обработки персональной информации Пользователей

7. МАУДО «ДПШ» собирает и хранит только ту персональную информацию, которая необходима для предоставления услуг Сайта или исполнения соглашений и договоров с Пользователем, за исключением случаев, когда законодательством предусмотрено обязательное хранение информации в течение определенного законом срока.

8. Персональную информацию Пользователя Сайта МАУДО «ДПШ» обрабатывает в целях информационно-справочного обслуживания, осуществления заявок на обслуживание, реализации книги жалоб и предложений.

IV. Условия обработки персональной информации Пользователя, удаления и ее передачи третьим лицам

9. МАУДО «ДПШ» хранит персональную информацию Пользователя в соответствии с внутренними регламентами.

10. Персональная информация Пользователя, предоставленная через формы Сайта, не хранится на Сайте в сети Интернет, используется исключительно для предоставления услуги.

11. В отношении персональной информации Пользователя сохраняется ее конфиденциальность, исключен общий доступ неограниченному кругу лиц.

12. МАУДО «ДПШ» не предоставляет персональную информацию Пользователей Сайта третьим лицам, кроме случаев, когда этого прямо может требовать законодательство (например, по запросу суда).

13. Удаление персональной информации происходит по письменному обращению Пользователя или его законного представителя в МАУДО «ДПШ».

14. При обработке персональной информации Пользователя МАУДО «ДПШ» руководствуется Федеральным законом №152-ФЗ «О персональных данных».

V. Обработка персональной информации при помощи файлов Cookie и счетчиков

15. Файлы cookie, передаваемые Сайтом оборудованию Пользователя и оборудованием Пользователя Сайта, могут использоваться МАУДО «ДПШ» в статистических и исследовательских целях, а также для улучшения разделов Сайта.

16. Пользователь осознает, что оборудование и программное обеспечение, используемые им для посещения Сайта в сети Интернет могут обладать функцией запрета операций с файлами cookie (для любых сайтов или для определенных сайтов), а также удаления ранее полученных файлов cookie.

17. МАУДО «ДПШ» вправе установить, что предоставление определенного раздела Сайта возможно лишь при условии, что прием и получение файлов cookie разрешены Пользователем.

18. Структура файлов cookie, его содержание и технические параметры определяются МАУДО «ДПШ» и могут изменяться без предварительного уведомления Пользователя.

19. Счетчики, размещенные МАУДО «ДПШ» на Сайте, могут использоваться для анализа файлов cookie Пользователя, для сбора и обработки статистической информации об использовании Сайта, а также для обеспечения работоспособности Сайта в целом или их отдельных функций в частности. Технические параметры работы счетчиков определяются МАУДО «ДПШ» и могут изменяться без предварительного уведомления Пользователя.

VI. Меры, применяемые для защиты персональной информации пользователя

20. МАУДО «ДПШ» принимает необходимые и достаточные организационные и технические меры для защиты персональной информации Пользователя от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий с ней третьих лиц.

VII. Изменение Политики конфиденциальности. Применимое законодательство

21. МАУДО «ДПШ» имеет право вносить изменения в настоящую Политику конфиденциальности. При внесении изменений в актуальной редакции указывается дата последнего обновления. Новая редакция вступает в силу с момента ее размещения, если иное не предусмотрено новой редакцией Политики. Действующая редакция постоянно доступна на странице по адресу www.chel-dpsh.ru.

22. К настоящей Политике и отношениями между Пользователем и МАУДО «ДПШ», возникающими в связи с применением Политик конфиденциальности, подлежит применении право Российской Федерации.

VIII. Обратная связь, вопросы и предложения

23. Все предложения или вопросы по поводу настоящей Политики Пользователь вправе направить по адресу: 454080, г. Челябинск, Свердловский пр., д.59.

Приложение 3
к приказу МАУДО «ДПШ»
от 19.01.26 № 22-од

Пользовательское соглашение МАУДО «ДПШ»

I. Общие положения

1. Муниципальное автономное учреждение дополнительного образования «Дворец пионеров и школьников им. Н.К. Крупской г. Челябинска» (далее — МАУДО «ДПШ») предоставляет пользователю сайта (далее – Пользователь) доступ к сайту, расположенный по адресу в сети интернет www.chel-dpsh.ru. На условиях, изложенных в настоящем Пользовательском соглашении (далее — «Соглашение»). Соглашение вступает в силу с момента выражения Пользователем согласия с его условиями в порядке, предусмотренном п.4 Соглашения.

2. МАУДО «ДПШ» предоставляет Пользователям доступ к разделам сайта, включая возможность оставлять комментарии под разделами сайта. Все существующие на данный момент разделы, а также любое развитие их и/или добавление новых является предметом настоящего Соглашения.

3. Использование Сайта регулируется настоящим Соглашением, Политикой конфиденциальности, Политикой в отношении обработки и защиты персональных данных. Соглашение может быть изменено МАУДО «ДПШ» без какого-либо специального уведомления. Новая редакция Соглашения вступает в силу с момента ее размещения в сети Интернет по указанному в п.1 адресу, если иное не предусмотрено новой редакцией Соглашения. Действующая редакция Соглашения всегда находится на странице по адресу www.chel-dpsh.ru.

4. Начиная использовать какой-либо сервис/его отдельные функции, Пользователь считается принявшим условия Соглашения в полном объеме, без всяких оговорок и исключений. В случае несогласия Пользователя с какими-либо из положений Соглашения, Пользователь не вправе использовать сайт МАУДО «ДПШ». В случае если МАУДО «ДПШ» внес какие-либо изменения в Соглашение в порядке, предусмотренным п.3 данного Соглашения, с которыми Пользователь не согласен, он обязан прекратить использование сайта МАУДО «ДПШ».

II. Учетная запись Пользователя

5. Персональная информация Пользователя, содержащаяся в учетной записи Пользователя, хранится и обрабатывается МАУДО «ДПШ» в соответствии с условиями Политики конфиденциальности.

III. Условия использования сайта.

6. Пользователь самостоятельно несет ответственность перед третьими лицами за свои действия, связанные с использованием Сайта, в том числе, если такие

действия приведут к нарушению прав и законных интересов третьих лиц, а также за соблюдение законодательства при использовании Сайта.

7. При использовании Сайта Пользователь не вправе:

1) нарушать права третьих лиц и/или причинять им вред в любой форме;

2) выдавать себя за другого человека или представителя организации и/или сообщества без достаточных на то прав, за администрацию или владельцев Сайта, а также применять любые другие формы и способы незаконного представительства других лиц в сети, а также вводить пользователей в заблуждение относительно свойств и характеристик каких-либо субъектов или объектов;

3) посылать, передавать или любым другим способом размещать и/или распространять контент при отсутствии прав на такие действия согласно законодательству или каким-либо договорным отношениям;

4) не санкционировано собирать и хранить персональные данные других пользователей;

5) нарушать нормальную работу Сайта;

6) содействовать действиям, направленным на нарушение ограничений и запретов, налагаемых Соглашением;

7) другим образом нарушать нормы законодательства, в том числе нормы международного права.

IV. Форма входа в личный кабинет абонента

8. Форма входа в личный кабинет Пользователя предназначена для авторизации в системе управления услугами, предоставляемыми оператором связи для абонента.

9. Персональная информация Пользователя, содержащаяся в форме входа в личный кабинет абонента, хранится на сайте и обрабатывается в соответствии с условиями Политики в отношении обработки и защиты персональных данных.

10. При заполнении формы входа в личный кабинет абонента Пользователь указывает логин и пароль. В дальнейшем авторизация и управление услугами осуществляется на сервере оператора. Предоставляемая и получаемая Пользователем информация передается по открытым каналам связи сети Интернет в защищенном виде по протоколу HTTPS.

11. Пользователь самостоятельно несет ответственность за все действия (а также их последствия) в рамках или с использованием Сайта.

V. Заполнение форм

12. Персональная информация Пользователя, содержащаяся в форме на оставление комментария, хранится на сайте и не обрабатывается в МАУДО «ДПШ» в соответствии с условиями Политики в отношении обработки и защиты персональных данных МАУДО «ДПШ».

13. При заполнении формы на оставление комментария Пользователь указывает свое имя, адрес электронной почты и самого сообщения. Предоставленная

информация передается по открытым каналам связи сети Интернет в защищенном виде по протоколу HTTPS.

14. Заполнение формы входа в личный кабинет.

14.1. Персональная информация Пользователя не хранится на сайте и обрабатывается в соответствии с условиями Политики в отношении обработки и защиты персональных данных.

14.2. При заполнении формы входа в личный кабинет Пользователь указывает логин и пароль.

14.3. Пользователь самостоятельно несет ответственность за все действия (а также их последствия) в рамках или с использованием Сайта.

VI. Отсутствие гарантий, ограничение ответственности

15. Пользователь использует Сайт на свой собственный риск. Сайт предоставляется «как есть».

16. Сайт не гарантирует, что соответствует или будет соответствовать требованиям Пользователя; разделы будут предоставляться непрерывно, быстро, надежно и без ошибок; результаты, которые будут получены с использованием разделов, будут точными и надежными и могут использоваться для каких-либо целей или в каком-либо качестве; качество какого-либо продукта, услуги, информации и пр., полученных с использованием сервисов, будет соответствовать ожиданиям Пользователя.

17. Любая информация и/или материалы, доступ к которым Пользователь получает с использованием Сайта, Пользователь может использовать на свой собственный страх и риск и самостоятельно несет ответственность за возможные последствия использования указанной информации и/или материалов, в том числе за ущерб, который это может причинить компьютеру Пользователя или третьим лицам, за потерю данных или любой другой вред.

18. Сайт не несет ответственности за любые виды убытков, произошедшие вследствие использования Пользователем Сайта или отдельных частей/функций/разделов Сайта.

VII. Иные положения

19. Настоящее Соглашение представляет собой договор между Пользователем и Сайтом относительно порядка использования Сайта и заменяет собой все предыдущие соглашения между Пользователем и Сайтом.

20. Настоящее Соглашение регулируется и толкуется в соответствии с законодательством Российской Федерации. Вопросы, не урегулированные настоящим Соглашением, подлежат разрешению в соответствии с законодательством Российской Федерации. Все возможные споры, вытекающие из отношений, регулируемых настоящим Соглашением, разрешаются в порядке, установленном действующим законодательством Российской Федерации, по нормам российского права. Везде по тексту настоящего Соглашения, если явно не указано иное, под термином

«законодательство» понимается как законодательство Российской Федерации, так и законодательство места пребывания Пользователя.

21. Ввиду безвозмездности услуг, оказываемых в рамках настоящего Соглашения, нормы о защите прав потребителей, предусмотренные законодательством Российской Федерации, не могут быть применены к отношениям между Пользователем и Сайтом.

22. Если по тем или иным причинам одно или несколько положений настоящего Соглашения будут признаны недействительными или не имеющими юридической силы, это не оказывает влияния на действительность или применимость остальных положений Соглашения.

Приложение 4
к приказу МАУДО «ДПШ»
от 19.01.26 № 22-09

Перечень
персональных данных, обрабатываемых в МАУДО «ДПШ»

№ п/п	Наименование категории субъекта персональных данных	Категории персональных данных субъекта
1.	Работники	1. фамилия, имя, отчество; 2. ИНН; 3. СНИЛС (№ страхового пенсионного свидетельства); 4. табельный номер; 5. пол; 6. номер, дата трудового договора; 7. дата рождения; 8. место рождения; 9. гражданство; 10. образование (среднее (полное) общее, начальное профессиональное, среднее профессиональное, высшее профессиональное, аспирантура, адъюнктура, докторантура); 11. наименование образовательного учреждения; 12. наименование, серия, номер, дата выдачи, направление или специальность, код по ОКСО, ОКИН документа об образовании, о квалификации или наличии специальных знаний 13. профессия (в т.ч. код по ОКПДТР); 14. стаж работы; 15. состояние в браке; 16. состав семьи, с указанием степени родства, фамилии, имени, отчества, года рождения ближайших родственников; 17. данные документа, удостоверяющего личность (вид, серия, номер, дата выдачи, наименование органа, выдавшего документ); 18. адрес и дата регистрации;

№ п/п	Наименование категории субъекта персональных данных	Категории персональных данных субъекта
		19. фактический адрес места жительства; 20. телефон; 21. сведения об отношении к воинской службе; 22. дата приема на работу; 23. характер работы; 24. вид работы (основной, по совместительству); 25. структурное подразделение; 26. занимаемая должность (специальность, профессия), разряд, класс (категория) квалификации; 27. ранее занимаемая должность; 28. тарифная ставка (оклад), надбавка, руб. 29. основание трудоустройства; 30. личная подпись работника; 31. электронная подпись; 32. сведения об аттестации (дата, решение, номер и дата документа, основание); 33. сведения о профессиональной подготовке (дата начала и окончания переподготовки, специальность (направление, профессия, наименование, номер, дата документа, свидетельствующего о переподготовке, основание переподготовки); 34. сведения о наградах, поощрениях, почетных званиях (наименование, номер, дата награды); 35. сведения об отпусках (вид, период работы, количество дней, дата начала и окончания, основание); 36. сведения о социальных льготах, на которые работник имеет право в соответствии с законодательством (наименование льготы, номер, дата выдачи документа, основание); 37. сведения об увольнении (основания, дата, номер и дата приказа); 38. объем работы; 39. сведения о доходах; 40. сведения из трудовой книжки; 41. сведения из личной медицинской книжки;

№ п/п	Наименование категории субъекта персональных данных	Категории персональных данных субъекта
		42. сведения из водительского удостоверения; 43. место работы; 44. адрес электронной почты; 45. номер банковской карты; 46. номер лицевого счета; 47. фотография.
2.	Ближайшие родственники работников	1. фамилия, имя, отчество; 2. степень родства; 3. год рождения.
3.	Бывшие работники	1. фамилия, имя, отчество; 2. ИНН; 3. СНИЛС (№ страхового пенсионного свидетельства); 4. номер, дата трудового договора; 5. дата рождения; 6. место рождения; 7. данные документа, удостоверяющего личность (вид, серия, номер, дата выдачи, наименование органа, выдавшего документ); 8. дата приема на работу; 9. характер работы; 10. вид работы (основной, по совместительству); 11. структурное подразделение; 12. занимаемая должность (специальность, профессия), разряд, класс (категория) квалификации; 13. тарифная ставка (оклад), надбавка, руб.; 14. основание трудоустройства; 15. сведения об отпусках (вид, период работы, количество дней, дата начала и окончания, основание); 16. сведения о социальных льготах, на которые работник имеет право в соответствии с

№ п/п	Наименование категории субъекта персональных данных	Категории персональных данных субъекта
		законодательством (наименование льготы, номер, дата выдачи документа, основание); 17. сведения об увольнении (основания, дата, номер и дата приказа); 18. объем работы; 19. сведения о доходах; 20. номер банковской карты; 21. номер лицевого счета; 22. фотография.
4.	Соискатели	1. фамилия, имя, отчество; 2. образование; 3. специальность; 4. профессия; 5. предыдущий опыт работы; 6. стаж по специальности; 7. контактный телефон; 8. адрес электронной почты.
5.	Педагоги – члены рабочих групп, экспертных советов, оргкомитета, жюри	1. фамилия, имя, отчество; 2. наименование учреждения; 3. должность; 4. контактный телефон.
6.	Обучающиеся	1. фамилия, имя, отчество; 2. дата рождения; 3. место рождения; 4. пол; 5. класс; 6. сведения о посещаемости занятий; 7. контактный телефон; 8. электронная почта;

№ п/п	Наименование категории субъекта персональных данных	Категории персональных данных субъекта
		9. данные о состоянии здоровья; 10. данные об инвалидности; 11. фотография; 12. данные документа, удостоверяющего личность (вид, серия, номер, дата выдачи, наименование органа, выдавшего документ); 13. ИНН; 14. СНИЛС (№ страхового пенсионного свидетельства); 15. автобиография; 16. домашний адрес; 17. домашний телефон; 18. страница в социальной сети; 19. наличие знания языков; 20. хобби; 21. наименование образовательной организации; 22. наименование секции; 23. сведения о полученных наградах и достижениях; 24. сведения о родителях (законных представителях).
7.	Родители (законные представители) обучающихся	1. фамилия, имя, отчество; 2. данные документа, удостоверяющего личность (вид, серия, номер, дата выдачи, наименование органа, выдавшего документ); 3. домашний адрес; 4. место работы; 5. должность; 6. контактный телефон; 7. личная подпись.
8.	Физические лица, состоящие в гражданско-	1. фамилия, имя, отчество; 2. адрес регистрации ИП;

№ п/п	Наименование категории субъекта персональных данных	Категории персональных данных субъекта
	правовых отношениях	3. домашний адрес; 4. ИНН; 5. ОГРН; 6. номер расчетного счета; 7. название банка; 8. контактный телефон.

Приложение 5
к приказу МАУДО «ДПШ»
от 19.01.26 № 22-09

Положение
об обработке персональных данных с использованием средств автоматизации

I. Общие положения

1. Настоящее Положение об обработке персональных данных с использованием средств автоматизации (далее — Положение) Муниципального автономного учреждения дополнительного образования «Дворец пионеров и школьников им Н.К. Крупской г. Челябинска» (далее - МАУДО «ДПШ») разработано в соответствии с Конституцией Российской Федерации от 25.12.1993, Трудовым кодексом Российской Федерации от 30.12.2001 №197-ФЗ, Гражданским кодексом Российской Федерации от 30.11.1994 №51-ФЗ, Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27.07.2006 №149-ФЗ, Федеральным законом «О персональных данных» от 27.07.2006 №152-ФЗ, Постановлением Правительства Российской Федерации «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 №1119, а также другими нормативно-правовыми актами, действующими на территории Российской Федерации.

2. Цели разработки Положения:

2.1. Определение порядка обработки персональных данных субъектов персональных данных, персональные данные которых подлежат обработке на основании полномочий МАУДО «ДПШ».

2.2. Обеспечение защиты прав и свобод человека и гражданина при обработке их персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

2.3. Установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

3. К любой информации, содержащей персональные данные субъекта, применяется режим конфиденциальности, за исключением:

- обезличенных персональных данных;
- общедоступных персональных данных.

4. Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении срока их хранения, или продлевается на основании заключения экспертной комиссии МАУДО «ДПШ», если иное не определено законом Российской Федерации.

II. Термины и определения

5. **Доступ к информации** – возможность получения информации и ее использования.

Информационная система (ИС) – система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию.

Информация – сведения (сообщения, данные) независимо от формы их представления (ст.2 Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и защите информации»).

Носитель информации – любой материальный объект или среда, используемый для хранения или передачи информации.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных (ст.3 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»).

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных (ст.3 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»).

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными ст.3 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»).

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (ст.3 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»).

Средство защиты информации (СЗИ) – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Субъект персональных данных – физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных.

III. Порядок использования персональных данных

6. Обработка персональных данных может осуществляться исключительно в целях, указанных в Политике обработки и защиты персональных данных МАУДО «ДПШ».

7. При определении объема и содержания, обрабатываемых персональных данных работники МАУДО «ДПШ» должны руководствоваться Политикой обработки и защиты персональных данных МАУДО «ДПШ» с учетом действующего законодательства Российской Федерации, а также настоящим Положением.

8. Обработка персональных данных с использованием средств автоматизации (автоматизированным способом) может осуществляться исключительно на автоматизированных рабочих местах ИСПДн утверждённых «Перечнем автоматизированных рабочих мест информационных систем персональных данных».

IV. Порядок хранения персональных данных

9. Хранение носителей (дискет, дисков и т.п.), содержащих персональные данные, должно осуществляться в специальных папках, закрытых шкафах или сейфах, в порядке, исключающем доступ к ним третьих лиц.

10. Безопасность персональных данных при их обработке с использованием технических и программных средств обеспечивается с помощью системы защиты персональных данных, включающей в себя организационные меры и средства защиты информации, удовлетворяющие устанавливаемым в соответствии с законодательством РФ требованиям, обеспечивающим защиту информации.

11. Обработка персональных данных в МАУДО «ДПШ» осуществляется до наступления одного из условий прекращения обработки персональных данных указанных в Политике обработки и защиты персональных данных МАУДО «ДПШ». Перечень нормативно-правовых актов, определяющих основания обработки персональных данных в МАУДО «ДПШ» определяется «Перечнем сведений, содержащих персональные данные и правовые основания обработки персональных данных».

12. По истечении срока хранения (30 дней, если иное не прописано в нормативно-правовых актах) для машинных носителей допускается гарантированное удаление информации методом многократной перезаписи с помощью специализированных программ (например, «Safe Erase», «Eraser», «FDelete») без уничтожения материального носителя.

13. Обезличивания персональных данных в МАУДО «ДПШ» не предполагается.

V. Порядок передачи персональных данных

14. Передавать персональные данные субъектов допускается только тем работникам, которые имеют допуск к обработке персональных данных.

15. В целях соблюдения законодательства РФ, для достижения целей обработки, а также в интересах и с согласия субъектов персональных данных МАУДО «ДПШ» в ходе своей деятельности предоставляет персональные данные организациям, перечисленным в Политике обработки и защиты персональных данных МАУДО «ДПШ».

VI. Организация защиты персональных данных

16. Защита персональных данных субъекта от неправомерного их использования или утраты обеспечивается МАУДО «ДПШ» за счет своих средств.

17. Защита персональных данных должна вестись по трём взаимодополняющим направлениям:

17.1. Проведение организационных мероприятий:

1) разработка и внедрение внутренних организационно-распорядительных документов, регламентирующих обработку и защиту персональных данных субъектов, в том числе порядок доступа в помещения и к персональным данным;

2) ознакомление работников с законодательством Российской Федерации и внутренними нормативными документами, получение обязательств, касающихся обработки персональных данных;

3) организация учёта носителей персональных данных;

4) разработка модели угроз безопасности персональным данным;

5) проведение обучения работников по вопросам защиты персональных данных.

17.2. Программно-аппаратная защита – внедрение программно-аппаратных средств защиты информации, прошедших в соответствии с Федеральным законом №184 от 27.12.2002 г. «О техническом регулировании» оценку соответствия.

17.3. Инженерно-техническая защита:

1) установка сейфов или запирающихся шкафов для хранения носителей персональных данных;

2) установка усиленных дверей, сигнализации, режима охраны здания и помещений, в которых обрабатываются персональные данные.

18. Определение конкретных мер, общую организацию, планирование и контроль выполнения мероприятий по защите персональных данных осуществляет ответственный за организацию обработки персональных данных в соответствии с законодательством в области защиты персональных данных и локальными нормативно-правовыми актами МАУДО «ДПШ».

19. Организацию и контроль защиты персональных данных в структурных подразделениях МАУДО «ДПШ» осуществляют их непосредственные руководители в соответствии с Положением по проведению внутреннего контроля соответствия обработки персональных данных с требованиями к защите персональных данных.

VII. Порядок предоставления доступа к персональным данным

20. Допуск к персональным данным субъекта могут иметь только те работники МАУДО «ДПШ», которым персональные данные необходимы в связи с исполнением ими своих трудовых обязанностей. Перечень таких работников отражен в «Списке лиц, доступ которых к персональным данным необходим для выполнения служебных (трудовых) обязанностей».

21. Процедура оформления допуска к персональным данным представляет собой следующую строгую последовательность действий:

1) ознакомление работника с настоящим Положением, Политикой обработки и защиты персональных данных МАУДО «ДПШ» и другими локальными нормативно-правовыми актами МАУДО «ДПШ», касающимися обработки персональных данных;

2) истребование с работника «Обязательства о неразглашении информации ограниченного доступа».

22. Каждый работник должен иметь доступ к минимально необходимому набору персональных данных субъектов, необходимых ему для выполнения служебных (трудовых) обязанностей.

23. Работникам, не имеющим надлежащим образом оформленного допуска, доступ к персональным данным субъектов запрещается.

VIII. Требования по обеспечению безопасности

24. Состав информационных систем МАУДО «ДПШ» определяется «Перечнем информационных систем».

25. Под техническими средствами, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных, программные средства, средства защиты информации, применяемые в информационных системах.

26. Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

27. Средства защиты информации, применяемые в информационных системах, в обязательном порядке проходят процедуру оценки соответствия в установленном законодательством РФ порядке.

28. Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер, а также применения технических и (или) программных средств.

29. Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

30. Безопасность персональных данных при их обработке в информационной системе обеспечивает специалист, ответственный за обеспечение безопасности персональных данных в информационных системах.

31. При обработке персональных данных в информационной системе должно быть обеспечено:

1) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

2) своевременное обнаружение фактов несанкционированного доступа к персональным данным;

3) недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

4) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

5) постоянный контроль над обеспечением уровня защищенности персональных данных.

32. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают:

1) определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

2) разработку на основе модели угроз системы защиты информации, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

3) проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

4) установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

5) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

6) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

7) учет лиц, допущенных к работе с персональными данными в информационной системе;

8) контроль по соблюдению условий использования средств защиты информации, предусмотренных эксплуатационной и технической документации;

9) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

10) описание системы защиты персональных данных.

33. Иные требования по обеспечению безопасности информации и средств защиты информации в МАУДО «ДПШ» выполняются в соответствии с требованиями федеральных органов исполнительной власти и органов исполнительной власти субъекта РФ, в котором находится Оператор.

IX. Ответственность

34. Ответственность за соблюдение требований по защите информации ограниченного доступа и надлежащего порядка проводимых работ возлагается на пользователей ИС, ответственного за обеспечение безопасности персональных данных в информационных системах и ответственного за организацию обработки персональных данных МАУДО «ДПШ».

35. Работники МАУДО «ДПШ», виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

36. Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе другим работникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных настоящим Положением, локальными нормативно-правовыми актами МАУДО «ДПШ», влечет наложение на работника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Работник МАУДО «ДПШ», имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба МАУДО «ДПШ» (в соответствии с п.7 ст.243 Трудового кодекса РФ).

В отдельных случаях, при разглашении персональных данных, работник, совершивший указанный проступок, несет ответственность в соответствии со статьей 13.14 Кодекса об административных правонарушениях РФ.

37. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии со ст.137 Уголовного кодекса РФ.

38. Директор МАУДО «ДПШ» за нарушение норм, регулирующих получение, обработку и защиту персональных данных субъектов, несет административную ответственность согласно ст.5.27 и 5.39 Кодекса об административных правонарушениях Российской Федерации, а также возмещает субъекту ущерб, причиненный неправомерным использованием информации, содержащей персональные данные этого субъекта.

Приложение 6
к приказу МАУДО «ДПШ»
от 12.01.26 № 22-09

Положение
о порядке обработке персональных данных
без использования средств автоматизации

I. Общие положения

1. Правила обработки персональных данных, осуществляемой без использования средств автоматизации Муниципального автономного учреждения дополнительного образования «Дворец пионеров и школьников им Н.К. Крупской г. Челябинска» (далее - МАУДО «ДПШ»), установленные настоящим Положением, должны применяться с учетом требований постановления Правительства Российской Федерации «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15 сентября 2008 г. №687, а также требований нормативных правовых актов федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации.

II. Термины и определения

2. **Несанкционированный доступ (НСД)** - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами (ФСТЭК. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) Москва 2001).

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (ст.3 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»).

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных (ст.3 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»).

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение

персональных данных (ст.3 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»).

Обработка персональных данных без использования средств автоматизации – обработка персональных данных, при которой такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека (Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утв. постановлением Правительства РФ от 15.09.2008 №687).

Субъект персональных данных – физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных.

Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных (ст.3 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»).

III. Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации

3. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее - материальные носители), в специальных разделах или на полях форм (бланков).

4. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

5. Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе работники МАУДО «ДПШ» или лица, осуществляющие такую обработку по договору с МАУДО «ДПШ»), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется МАУДО «ДПШ» без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами МАУДО «ДПШ».

6. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:

1) типовая форма или связанные с ней документы должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, наименование и адрес МАУДО «ДПШ», фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых МАУДО «ДПШ» способов обработки персональных данных;

2) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных;

3) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных.

7. При ведении журналов (журналов регистрации, журналов посещений), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных в помещение МАУДО «ДПШ» или в иных аналогичных целях, должны соблюдаться следующие условия:

1) необходимость ведения такого журнала должна быть предусмотрена актом МАУДО «ДПШ», содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных;

2) копирование содержащейся в таких журналах информации не допускается;

3) персональные данные каждого субъекта персональных данных могут заноситься в такой журнал не более 1 (одного) раза в каждом случае пропуска субъекта персональных данных.

8. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, зачеркивание, стирание).

9. По истечении срока хранения (30 дней, если иное не прописано в нормативно-правовых актах) документы, либо иные материальные носители

персональных данных должны быть уничтожены без возможности восстановления (например, в бумагорезательных машинах) с составлением акта.

10. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем изготовления нового материального носителя с уточненными персональными данными.

IV. Особенности обеспечения безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации

11. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

12. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

13. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются приказом директора МАУДО «ДПШ».

V. Ответственность

14. Ответственность за соблюдение требований по защите информации ограниченного доступа и надлежащего порядка проводимых работ возлагается на пользователей ИС, ответственного за обеспечение безопасности персональных данных в информационных системах и ответственного за организацию обработки персональных данных МАУДО «ДПШ».

15. Работники МАУДО «ДПШ», виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

15.1. Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе другим работникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных настоящим Положением, локальными нормативно-правовыми актами (приказами, распоряжениями) МАУДО «ДПШ», влечет наложение на работника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде:

замечания, выговора, увольнения. Работник МАУДО «ДПШ», имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба МАУДО «ДПШ» (в соответствии с п.7 ст. 243 Трудового кодекса РФ).

В отдельных случаях, при разглашении персональных данных, работник, совершивший указанный проступок, несет ответственность в соответствии со статьей 13.14 Кодекса об административных правонарушениях РФ.

15.2. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии со ст. 137 Уголовного кодекса РФ.

16. Директор МАУДО «ДПШ» за нарушение норм, регулирующих получение, обработку и защиту персональных данных субъектов, несет административную ответственность согласно ст. 5.27 и 5.39 Кодекса об административных правонарушениях Российской Федерации, а также возмещает субъекту ущерб, причиненный неправомерным использованием информации, содержащей персональные данные этого субъекта.

Приложение 7
к приказу МАУДО «ДПШ»
от 19.01.26 № 22-09

Правила
обработки персональных данных

I. Общие положения

1. Данные Правила разработаны с целью защиты интересов Муниципального автономного учреждения дополнительного образования «Дворец пионеров и школьников им. Н.К. Крупской г. Челябинска» (далее - МАУДО «ДПШ») и субъектов персональных данных, в целях предотвращения раскрытия (передачи), а также соблюдения надлежащих правил обращения с персональными данными.

2. Данные Правила предназначены для использования всеми работниками МАУДО «ДПШ», допущенными к работе с персональными данными.

3. Работники МАУДО «ДПШ», доступ которых к персональным данным необходим для выполнения ими своих служебных (трудовых) обязанностей, должны быть ознакомлены с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных

II. Термины и определения

4. **Информация** - сведения (сообщения, данные) независимо от формы их представления (ст.2 Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и защите информации»).

Доступ к информации – возможность получения информации и её использования (ст.2 Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и защите информации»).

Носитель информации - любой материальный объект или среда, используемый для хранения или передачи информации.

Несанкционированный доступ (НСД) – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т.д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т.д. различных организаций путём изменения (повышения, фальсификации) своих прав доступа.

Информационная система (ИС) – система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т.д.), которые обеспечивают и распространяют информацию.

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными,

включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных (ст.3 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»).

Пароль – секретная комбинация цифр, знаков, слов, или осмысленное предложение, служащие для защиты информации от несанкционированного доступа к информационным ресурсам.

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (ст.3 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»).

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц (ст.3 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»).

Субъект персональных данных — физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных

Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных (ст.3 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»).

III. Порядок работы со сведениями, содержащими персональные данные

5. При обработке персональных данных на бумажных носителях, съёмных носителях (дискетах, дисках, флеш-носителях и т.п.), компьютерах и других технических средствах, работники МАУДО «ДПШ» обязаны следить как за сохранностью самих бумажных документов, съёмных носителей и компьютеров и других технических средств, так и за сохранностью содержащейся в них информации, а именно не допускать неправомерного ознакомления с ней лиц, не имеющих допуска к работе с персональными данными.

6. Запрещается хранение или оставление бумажных документов и съёмных носителей, содержащих персональные данные, в виде, позволяющем осуществить визуальный просмотр содержащихся в них персональных данных, их фотографирование или несанкционированное создание копий. Напечатанные документы, содержащие персональные данные, должны изыматься из принтеров немедленно. Хранение бумажных документов и съёмных носителей, содержащих персональные данные, допускается только в специальных закрытых шкафах, сейфах и помещениях, к которым исключён доступ лиц, не допущенных к обработке соответствующих персональных данных.

7. Запрещается без прямой служебной необходимости делать выписки персональных данных, распечатывать документы с персональными данными или записывать персональные данные на съёмные носители.

8. Запрещается использовать для передачи персональных данных съёмные носители, не учтённые в «Журнале учета съемных носителей информации».

9. Запрещается выносить документы, съёмные носители или переносные компьютеры, содержащие персональные данные, за пределы служебных помещений МАУДО «ДПШ», если это не требуется для выполнения служебных (трудовых) обязанностей и если на это не дано разрешение директора МАУДО «ДПШ» или ответственного за организацию обработки персональных данных.

10. Бумажные документы с персональными данными, у которых истёк срок хранения, лишние или испорченные копии документов с персональными данными, должны быть уничтожены без возможности их восстановления (например, в шредерах).

11. Большие объёмы бумажных документов с персональными данными, съёмные носители с персональными данными, а также встроенные в компьютеры носители с персональными данными должны уничтожаться под контролем ответственного за организацию обработки персональных данных, способом, исключающим дальнейшее восстановление информации.

12. Мониторы компьютеров, использующихся для обработки персональных данных, должны быть ориентированы таким образом, чтобы исключить визуальный просмотр информации с них лицами, не имеющими допуск к обработке персональных данных.

13. Запрещается установка и использование при работе в АРМ вредоносных программ, ведущих к блокированию работы сети, самовольное изменение сетевых адресов, самовольное вскрытие блоков АРМ, модернизация или модификация АРМ и программного обеспечения. Несанкционированная передача АРМ с прописанными сетевыми настройками. Передача АРМ из одного подразделения в другое производится только ответственным за обеспечение безопасности информации с предварительно удаленными сетевыми настройками. Использование технологии беспроводного доступа без разрешения ответственного за обеспечение безопасности в информационных системах.

14. Для работы с персональными данными разрешается использовать только автоматизированные рабочие места, указанные в «Перечне автоматизированных рабочих мест информационных систем», при этом для обработки персональных данных можно использовать только программное обеспечение, указанное в «Перечне общесистемного и прикладного программного обеспечения».

15. Запрещается упоминать в разговоре с третьими лицами сведения, содержащие персональные данные.

16. Запрещается в нерабочее время или за пределами служебных помещений упоминать в разговоре с кем-либо, включая любых работников МАУДО «ДПШ», сведения, содержащие персональные данные.

17. Запрещается обсуждать порядок доступа, места хранения, средства и методы защиты персональных данных с кем-либо, кроме ответственного за организацию обработки персональных данных, ответственного за обеспечение безопасности персональных данных в информационных системах, руководства, или лица, уполномоченного руководством на обсуждение данных вопросов.

IV. Порядок доступа лиц в помещения

18. При обеспечении доступа лиц соблюдаются требования законодательства РФ по защите персональных данных.

19. Обеспечение доступа лиц в помещения предусматривает комплекс специальных мер, направленных на поддержание и обеспечение установленного порядка деятельности структурных подразделений и определяет порядок пропуска работников МАУДО «ДПШ» и иных третьих лиц в помещения.

20. Контроль за порядком обеспечения доступа лиц в помещения возлагается на руководителя структурного подразделения.

21. Не допускается нахождение работников МАУДО «ДПШ» в помещениях в нерабочее для них время без согласования с руководством и без служебной записки. В нерабочее время, в случае служебной необходимости могут задержаться на рабочих местах только при наличии служебной записки, подписанной руководителем структурного подразделения. В служебной записке указывается (Ф.И.О. работника, № кабинета и время окончания работы, при работе нескольких человек указывается ответственное лицо). Служебная записка предоставляется ответственному за организацию обработки персональных данных. В случае неотложных заданий, поступивших после окончания рабочего дня, порядок допуска в служебные помещения осуществляется аналогичным образом, по личному разрешению ответственного за организацию обработки персональных данных до начала неотложных работ.

22. В случаях, не терпящих отлагательства (пожар, авария систем тепло-, водоснабжения и т.п.), когда находящимся в помещении оборудованию, материальным ценностям и документации грозит опасность уничтожения или вывода из строя, работник оповещает пожарную охрану (аварийную службу), вызывает руководителя подразделения или работника, ответственного за помещение. Служебное помещение вскрывается до прибытия указанных лиц, и принимаются меры к тушению пожара (ликвидации аварии), эвакуации ценностей, имущества и документации. Около эвакуируемых ценностей, имущества и документации выставляется временный пост охраны. Акт о вскрытии помещения составляется после окончания работ, связанных с ликвидацией происшествия.

23. Нахождение посетителей допускается только в рабочее время в присутствии работников имеющих допуск.

24. В помещения ИС пропускаются:

- беспрепятственно – директор МАУДО «ДПШ» и работники, имеющие допуск к работе с персональными данными и с целью выполнения должностных обязанностей;

- при наличии служебного удостоверения, с разрешения директора МАУДО «ДПШ» или руководителя структурного подразделения, в сопровождении ответственного за организацию обработки персональных данных или руководителя структурного подразделения – работники контролирующих органов, работники пожарных и аварийных служб, работники полиции;

- ограниченно – работники, не имеющие допуска к работе с персональными данными или не имеющие функциональных обязанностей в помещении, работники сторонних организаций и учреждений для выполнения договорных отношений.

25. Посетители пропускаются в помещения ИС МАУДО «ДПШ» в рабочее время в сопровождении работников, допущенных к обработке персональных данных.

26. В помещениях, в которых происходит обработка персональных данных, запрещено использование не предусмотренных служебными обязанностями технических устройств, фотографирование, видеозапись, звукозапись, в том числе с использованием мобильных телефонов.

27. Рабочие и специалисты ремонтно-строительных организаций пропускаются в помещение для проведения ремонтно-строительных работ на основании заявок, подписанных руководством МАУДО «ДПШ».

28. В целях предотвращения несанкционированного доступа к сведениям, содержащим персональные данные, работы проводятся только под контролем ответственного за организацию обработки персональных данных или руководителя структурного подразделения.

29. Контроль за допуском в служебные помещения в рабочее время возлагается на руководителей подразделений, за которыми закреплены данные помещения. В нерабочее время, выходные и нерабочие праздничные дни охрана служебных помещений обеспечивается средствами охранной сигнализации, а в случае их неисправности выставлением поста охраны.

30. Для исключения возможности бесконтрольного проникновения в помещения и к установленному в них оборудованию посторонних лиц, двери в отсутствие штатных работников запираются на ключ.

31. Помещения, где хранятся персональные данные, защищаемые криптографическими средствами защиты информации, должны быть оснащены входными дверьми с замками для обеспечения постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода. Помещения должны опечатываться по окончании рабочего дня или быть оборудованы соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии помещений.

32. Руководители структурных подразделений, либо работники, уполномоченные хранить ключи от сейфов и помещений, должны вести «Журнал учета ключей от сейфов и помещений».

33. Оборудование в помещении должно размещаться таким образом, чтобы исключить возможность бесконтрольного доступа к нему посторонних лиц.

34. Окна помещений, в которых ведётся обработка персональных данных, должны быть оборудованы шторами или жалюзи.

35. Режим работы охраны устанавливается штатным расписанием и должностными инструкциями.

36. Уборка помещений ИС должна производиться под контролем работника, допущенного к обработке персональных данных в этом помещении.

37. Во время уборки в помещении должна быть приостановлена работа с персональными данными, должны быть выключены или заблокированы все АРМ, на которых обрабатываются персональные данные. Носители, содержащие персональные данные, должны быть убраны в закрытые шкафы или сейфы.

V. Действия при обнаружении попыток несанкционированного доступа

38. К попыткам несанкционированного доступа относятся:

- сеансы работы с персональными данными незарегистрированных пользователей, или пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истёк, или превышающих свои полномочия по доступу к данным;

- действия третьего лица, пытающегося получить доступ (или уже получившего доступ) к ИС, при использовании учётной записи администратора или другого пользователя ИС, методом подбора пароля, использования личного пароля, разглашённого владельцем учётной записи или любым другим методом.

39. При выявлении факта несанкционированного доступа пользователь ИСПДн обязан:

1) прекратить несанкционированный доступ к персональным данным;

2) доложить директору МАУДО «ДПШ» служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;

3) известить руководителя структурного подразделения, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка несанкционированного доступа, о факте несанкционированного доступа;

4) известить ответственного за обеспечение безопасности персональных данных в информационных системах и ответственного за организацию обработки ПДн о факте несанкционированного доступа.

VI. Требования по техническому укреплению

40. Руководители структурных подразделений обеспечивают обязательное выполнение мероприятий по техническому укреплению и оборудованию специальными техническими средствами охраны, системами пожарной безопасности и должны руководствоваться следующими основными требованиями:

1) двери и окна должны иметь прочные и надежные петли, шпингалеты, крючки или задвижки и быть плотно подогнаны к рамам и дверным коробам. Допускается применение электромеханических, электромагнитных замков и задвижек;

2) оконные проемы первых этажей зданий должны быть укреплены металлическими решетками, запираемыми с внутренней стороны, если это не противоречит требованиям пожарной безопасности;

3) конструкция оконных рам должна исключать возможность демонтажа с наружной стороны оконного проема стекол;

4) стекла в рамах должны быть надежно закреплены в пазах;

5) рамы указанных оконных проемов должны оборудоваться запорными устройствами.

VII. Ответственность

41. Работники МАУДО «ДПШ», виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъектов, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

42. Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе другим работникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных локальными нормативно-правовыми актами (приказами, распоряжениями) МАУДО «ДПШ», влечет наложение на работника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Работник МАУДО «ДПШ», имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба МАУДО «ДПШ» (в соответствии с п.7 ст.243 Трудового кодекса РФ).

В отдельных случаях, при разглашении персональных данных, работник, совершивший указанный проступок, несет ответственность в соответствии со ст.13.14 Кодекса об административных правонарушениях РФ.

43. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии со ст.137 Уголовного кодекса РФ.

44. Директор МАУДО «ДПШ» за нарушение норм, регулирующих получение, обработку и защиту персональных данных субъектов, несет административную ответственность согласно ст.5.27 и 5.39 Кодекса об административных правонарушениях Российской Федерации, а также возмещает субъекту ущерб, причиненный неправомерным использованием информации, содержащей персональные данные этого субъекта.

Приложение 8
к приказу МАУДО «ДПШ»
от 19.01.26 № 22-ОД

Инструкция
по рассмотрению запросов субъекта персональных данных
или уполномоченного органа по защите прав
субъектов персональных данных

I. Общие положения

1. Настоящая Инструкция устанавливает отношения, возникающие при рассмотрении запросов субъектов персональных данных или Уполномоченного органа по защите прав субъектов персональных данных в Муниципальном автономном учреждении дополнительного образования «Дворец пионеров и школьников им. Н.К. Крупской г. Челябинска» (далее - МАУДО «ДПШ») в целях реализации обязательств, согласно требованиям статей 14, 20 и 21 Федерального закона «О персональных данных» от 27.07.2006 №152-ФЗ, Федерального закона от 02.05.2006 №59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации».

2. Положения настоящей Инструкции распространяются на действия работников МАУДО «ДПШ» при обращении субъектов либо при получении запроса субъекта персональных данных или его законного представителя, при обращении Уполномоченного органа по защите прав субъектов персональных данных.

II. Определения

3. **Персональные данные (далее – ПДн)** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Оператор ПДн – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Информационная система персональных данных (далее – ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Управление Роскомнадзора (далее – Роскомнадзор) – Уполномоченный орган по защите прав субъекта персональных данных.

III. Ответственность

4. Ответственность за реализацию положений данной Инструкции возложить в соответствии с Трудовым кодексом РФ, Кодексом об административных правонарушениях РФ на ответственного за организацию обработки персональных данных МАУДО «ДПШ».

IV. Действия работников при получении обращения (запроса, жалобы) субъектов ПДн

5. В случае поступления запроса об обработке персональных данных от субъекта ПДн или его законного представителя необходимо выполнить следующие действия:

1) уполномоченный работник МАУДО «ДПШ» проверяет запрос по требованиям п.3. ст.14 Федерального закона №152-ФЗ, и при соответствии производит регистрацию документа в Журнале учёта обращений субъектов. Затем запрос передается ответственному за обработку ПДн МАУДО «ДПШ», который должен в течение 30 дней с даты получения запроса (согласно п.1 ст.20 №152-ФЗ) подтвердить обработку ПДн в случае ее осуществления. Если обработка ПДн субъекта не ведется, то в течение 30 дней с даты получения запроса (согласно п.2 ст.20 №152-ФЗ). Форма запроса на наличие ПДн приведена в Приложении 2, а формы ответов на эти запросы в Приложении 6.

2) при получении запроса субъекта ПДн или его представителя на ознакомление с обрабатываемыми ПДн, необходимо в течение 30 дней с даты получения запроса (согласно п.1 ст.20 №152-ФЗ) предоставить для ознакомления ПДн субъекта. Если обработка ПДн субъекта не ведется, то в течение 30 дней с даты получения запроса (согласно п.2 ст.20 №152-ФЗ) необходимо отправить уведомление об отказе предоставления информации по ПДн. Форма запроса на наличие ПДн приведена в Приложении 2, а формы ответов на эти запросы в Приложении 6.

6. Субъект ПДн или его законный представитель имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей:

– подтверждение обработки ПДн, а также правовые основания и цели такой обработки;

– способы обработки ПДн;

– сведения о лицах, которые имеют доступ к ПДн;

– перечень обрабатываемых ПДн и источник их получения;

– сроки обработки ПДн, в том числе сроки их хранения.

6.1. При получении запроса субъекта ПДн или его представителя на уточнение ПДн необходимо внести в них необходимые изменения в срок, не превышающий 7 рабочих дней со дня предоставления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются неполными, неточными или неактуальными. Форма запроса на уточнение ПДн приведена в Приложении 3, а формы ответов на эти запросы в Приложении 7.

6.2. При получении запроса субъекта ПДн или его представителя на уничтожение ПДн, подтверждающих, что такие ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки (согласно п.3 ст.20 №152-ФЗ) необходимо их уничтожить в срок, не превышающий 7 рабочих дней. Форма запроса на уничтожение ПДн приведена в Приложении 4, а формы ответов на эти запросы в Приложении 8.

6.3. При получении запроса на отзыв согласия на обработку ПДн необходимо прекратить их обработку и, в случае, если сохранение ПДн более не требуется для

целей обработки персональных данных, уничтожить ПДн в срок, не превышающий 30 дней с даты поступления указанного отзыва (согласно п.5 ст.21 №152-ФЗ), если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между МАУДО «ДПШ» и субъектом персональных данных либо если МАУДО «ДПШ» не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами (согласно п.5 ст.21 №152-ФЗ). Форма запроса на отзыв согласия на обработку ПДн приведена в Приложении 5, а формы ответов на эти запросы в Приложении 9.

6.4. При выявлении неправомерной обработки ПДн МАУДО «ДПШ» при обращении или по запросу субъекта ПДн или его представителя необходимо в срок, не превышающий трех рабочих дней с даты этого выявления, прекратить неправомерную обработку ПДн (согласно п.3 ст.21 №152-ФЗ). В случае если обеспечить правомерность обработки персональных данных невозможно, МАУДО «ДПШ» в срок, не превышающий 10 рабочих дней с даты выявления неправомерной обработки персональных данных (согласно п.3 ст.21 №152-ФЗ), обязана уничтожить такие персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных МАУДО «ДПШ» обязана уведомить субъект ПДн или его представителя, а в случае, если обращение субъекта ПДн или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены Роскомнадзором, также уведомить указанный орган (Приложение 10).

6.5. При выявлении фактов неточности ПДн при обращении или по запросу субъекта ПДн или его представителя необходимо их блокировать с момента такого обращения или получения такого запроса на период проверки (согласно п. 1 ст. 21 №152-ФЗ). Если факт недостоверности ПДн подтвержден на основании сведений, представленных субъектом ПДн или его представителем, либо Роскомнадзором, необходимо уточнить ПДн в течение 7 рабочих дней со дня предоставления таких сведений и снять блокирование ПДн (согласно п.2 ст.21 №152-ФЗ) (Приложение 11).

6.6. При достижении целей обработки ПДн МАУДО «ДПШ» обязан незамедлительно прекратить обработку ПДн уничтожить соответствующие ПДн в срок, не превышающий 30 дней с даты достижения цели обработки ПДн (согласно п.4 ст.21 152ФЗ), если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между МАУДО «ДПШ» и субъектом персональных данных либо если МАУДО «ДПШ» не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами. Формы уведомления при достижении целей обработки ПДн приведены в Приложении 12.

7. В случае поступления запроса Роскомнадзора необходимо выполнить следующие действия:

7.1. МАУДО «ДПШ» обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных необходимую информацию в течение 30 дней с момента получения такого запроса (согласно п.4 ст.20 №152-ФЗ).

7.2. При выявлении неправомерных действий с ПДн при обращении или по запросу Уполномоченного органа по защите прав Субъекта ПДн необходимо прекратить неправомерную обработку в срок, не превышающий 3 рабочих дней, с

момента такого обращения или получения такого запроса на период проверки (согласно п.1 ст.21 №152-ФЗ). В случае невозможности обеспечения правомерности обработки МАУДО «ДПШ» ПДн в срок, не превышающий 10 рабочих дней с даты выявления неправомерности, незамедлительно прекратить обработку ПДн и уничтожить соответствующие ПДн в течение 30 дней с даты достижения цели обработки ПДн (согласно п.4 ст.21 152-ФЗ), если иное не предусмотрено договором, стороной которого является субъект персональных данных, иным соглашением между МАУДО «ДПШ» и субъектом персональных данных либо если МАУДО «ДПШ» не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами и отправить уведомление об уничтожении ПДн. Формы уведомления при выявлении неправомерности действий с ПДн приведены в Приложении 10.

7.3. При выявлении недостоверных ПДн при обращении или по запросу Роскомнадзора необходимо ПДн блокировать с момента такого обращения или получения такого запроса на период проверки (согласно п.1 ст.21 №152-ФЗ). Если факт недостоверности ПДн подтвержден на основании документов, предоставленных субъектом ПДн или его законным представителем, необходимо в течение 7 рабочих дней уточнить ПДн и снять их блокирование (согласно п. 2 ст. 21 №152-ФЗ). Если факт недостоверности ПДн не подтвержден, то необходимо отправить уведомление об отказе изменения и снять блокирование ПДн. Формы уведомления при выявлении недостоверности ПДн приведены в Приложении 11.

8. Прием запросов от субъектов ПДн или его законных представителей, а также от Уполномоченного органа по защите прав субъектов ПДн.

8.1. При получении запросов, перечисленных в разделе 6 настоящей Инструкции, уполномоченный работник МАУДО «ДПШ» регистрирует документ в соответствии с Федеральным законом №59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» и с утвержденной Инструкцией по ведению делопроизводства в МАУДО «ДПШ» и выполняет следующие действия:

1) в случае поступления запроса субъекта ПДн или его законного представителя необходимо зарегистрировать запрос и передать его ответственному за организацию обработки персональных данных для дальнейшего учета в «Журнале учёта обращений граждан (субъектов персональных данных) о выполнении их законных прав при обработке персональных данных»;

2) при личном обращении субъекта персональных данных в МАУДО «ДПШ», уполномоченный работник МАУДО «ДПШ» предоставляет форму запроса для заполнения субъектом ПДн (Приложения 2, 3, 4 и 5) или принимает запрос в произвольной форме. После принятия заполненной формы или запроса в произвольной форме работник МАУДО «ДПШ» сверяет сведения в запросе с предоставленными ему документами.

8.2. Необходимые сведения о персональных данных субъекта, которые должны присутствовать в запросе:

- фамилия, имя и отчество субъекта ПДн;
- номер основного документа, удостоверяющего личность субъекта ПДн или его законного представителя,
- сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных или его законного представителя и дата запроса.

В случае неправильно оформленного запроса или при отсутствии документов, удостоверяющих личность субъекта ПДн или его законного представителя, уполномоченный работник вправе отказать в приеме запроса и предложить сделать запрос в соответствии с требованиями п.3 ст.14. №152-ФЗ. При отказе субъекта ПДн или его законного представителя необходимо переделать запрос, уполномоченный работник МАУДО «ДПШ» делает об этом запись в журнале в соответствии с утвержденной инструкцией по ведению делопроизводства в МАУДО «ДПШ».

Если запрос оформлен в соответствии с требованиями законодательства, он принимается к обработке и передается ответственному за организацию обработки персональных данных.

8.3. В случае поступления запроса от Роскомнадзора необходимо данный запрос зарегистрировать в соответствии с утвержденной Инструкцией по ведению делопроизводства в МАУДО «ДПШ» и немедленно сообщить о запросе ответственному за организацию обработки персональных данных.

Приложение 1
к Инструкции по обработке запросов
субъекта персональных данных или
Уполномоченного органа по защите прав
субъектов персональных данных
в МАУДО «ДПШ»
от 19.01.26 № 22-09

Сводная таблица действий в ответ запросы субъекта по персональным данным

№	Запрос	Действия	Срок	Ответ
I. Запрос Субъекта ПДн или его представителя				
1.1	Наличие ПДн	Регистрация запроса и подтверждение обработки ПДн	30 дней (согласно п. 1 ст. 20 № 152-ФЗ)	Подтверждение обработки определенных категорий ПДн
		Отказ подтверждения обработки ПДн	30 дней (согласно п. 2 ст. 20 №152-ФЗ)	Уведомление об отказе подтверждения обработки ПДн
1.2	Ознакомление с ПДн	Предоставление информации по ПДн	30 дней (согласно п. 1 ст. 20 № 152-ФЗ)	1. Подтверждение факта обработки ПДн, а также правовые основания и цели такой обработки
				2. Цели и способы обработки ПДн
				3.Наименование и место нахождения оператора
				4. Сведения о лицах, которые имеют доступ к ПДн(кроме работников оператора)
				5. Перечень обрабатываемых ПДн и источник их получения
				6. Сроки обработки ПДн, в том числе сроки их хранения
				7. Наименование и адрес лица,

				осуществляющих обработку ПДн по поручению оператора, если обработка поручена или будет поручена такому лицу
				8. Информация об осуществлении или о предполагаемой трансграничной передаче данных
		Отказ предоставления информации по ПДн	30 дней (согласно п. 2 ст. 20 № 152-ФЗ)	Уведомление об отказе предоставления информации по ПДн
1.3	Уточнение ПДн	Изменение ПДн	7 рабочих дней со дня предоставления уточняющих сведений (согласно п.3 ст. 20 № 152-ФЗ)	Уведомление о внесенных изменениях
1.4.	Уничтожение ПДн	Уничтожение ПДн	7 рабочих дней со дня предоставления сведений о незаконном получении ПДн или отсутствии необходимости ПДн для заявленной цели обработки (согласно п. 3 ст. 20 №152-ФЗ)	Уведомление об уничтожении
1.5.	Отзыв согласия на обработку ПДн	Прекращение обработки и уничтожение ПДн	30 дней (согласно п. 5 ст. 21 №152-ФЗ)	Уведомление о прекращении обработки и уничтожении ПДн
		Отказ прекращения обработки и	30 дней (согласно	Уведомление об отказе прекращения

		уничтожения ПДн	п. 1 ст. 20 № 152-ФЗ)	обработки и уничтожения ПДн
1.6.	Недостоверность ПДн	Блокировка ПДн	С момента обращения субъекта ПДН о недостоверности или с момента получения запроса на период проверки (согласно п.1 ст. 21 №152-ФЗ)	Уведомление о внесенных изменениях
		Изменение ПДн	7 рабочих дней со дня предоставления уточненных сведений (согласно п.2 ст. 21 №152-ФЗ)	
		Снятие блокировки ПДн		
1.7	Неправомерная обработка ПДн	Прекращение неправомерной обработки ПДн	3 рабочих дня (согласно п.3 ст. 21 № 152-ФЗ)	Уведомление об устранении нарушений
		Уничтожение ПДн в случае невозможности обеспечения правомерности обработки	10 рабочих дней (согласно пункту 3 статьи 21 152-ФЗ)	Уведомление об уничтожении ПДн
1.8	Достижение целей обработки ПДн субъекта	Прекращение обработки ПДн Уничтожение ПДн	30 дней (согласно п. 4 ст.21 №152-ФЗ)	Уведомление об уничтожении ПДн
II. Запрос Уполномоченного органа по защите прав субъекта ПДн				
2.1	Информация для осуществления деятельности уполномоченного органа	Предоставление затребованной информации по ПДн	30 дней (согласно п. 4 ст. 20 152-ФЗ)	Предоставление затребованной информации

2.2	Недостоверность ПДн	Блокировка ПДн	С момента обращения Уполномоченного органа о недостоверности или с момента получения запроса на период проверки (согласно п. 1 ст. 21 №152-ФЗ)	Уведомление о внесенных изменениях
		Изменение ПДн	7 рабочих дней со дня предоставления уточненных сведений (согласно п.2 ст. 21 №152-ФЗ)	
		Снятие блокировки ПДн		
2.3	Неправомерность действий с ПДн субъекта	Прекращение неправомерной обработки ПДн	3 рабочих дня (согласно п. 3 ст.21 №152-ФЗ)	Уведомление об устранении нарушений
		Уничтожение ПДн в случае невозможности обеспечения правомерности обработки	10 рабочих дней (согласно п. 3 ст. 21 №152-ФЗ)	Уведомление об уничтожении ПДн
2.4	Достижение целей обработки ПДн субъекта	Блокировка ПДн	30 дней (согласно п. 4 ст. 21 №152-ФЗ)	Уведомление об уничтожении ПДн

Приложение 9
к приказу МАУДО «ДПШ»
от 19.01.26 № 22-09

Правила
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

1. Настоящими Правилами определяются процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных Требованиям к защите персональных данных при их обработке в информационных системах персональных данных, утвержденным постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119 (Собрание законодательства Российской Федерации, 2012, №45, ст.6257).

2. В целях осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в МАУДО «ДПШ» организовывается проведение плановых и внеплановых проверок условий обработки персональных данных на предмет соответствия Федеральному закону от 27.07.2006 №152-ФЗ «О персональных данных», принятым в соответствии с ним нормативным правовым актам и локальными актами МАУДО «ДПШ» (далее - Проверки).

3. Проверки проводятся в МАУДО «ДПШ» на основании ежегодного плана (плановые проверки) или на основании поступившего в МАУДО «ДПШ» письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки).

Ежегодный план проверок разрабатывается и утверждается комиссией по вопросам обеспечения безопасности информационных систем для осуществления внутреннего контроля соответствия обработки персональных данных требованиям, предусмотренным Федеральным законом «О персональных данных» (далее - Комиссия).

4. В плане по каждой проверке устанавливаются объект внутреннего контроля, проверяемый период, срок проведения проверки, ответственные исполнители.

5. Проверки проводятся Комиссией, создаваемой в соответствии с приказом МАУДО «ДПШ». В проведении проверки не может участвовать сотрудник, прямо или косвенно заинтересованный в ее результатах.

6. Основанием для проведения внеплановой проверки является поступившее в МАУДО «ДПШ» письменное обращение субъекта персональных данных или его представителя о нарушении правил обработки персональных данных.

7. Проведение внеплановой проверки организуется в течение пяти рабочих дней с момента поступления обращения.

8. Срок проведения проверки не может превышать месяц со дня принятия решения о ее проведении.

9. Члены Комиссии, получившие доступ к персональным данным субъектов персональных данных в ходе проведения проверки, обеспечивают конфиденциальность персональных данных субъектов персональных данных, не

раскрывают третьим лицам и не распространяют персональные данные без согласия субъекта персональных данных.

10. По результатам каждой проверки Комиссией проводится заседание. Решения, принятые на заседаниях Комиссии, оформляются протоколом.

11. По существу поставленных в обращении (жалобе) вопросов Комиссия в течение 5 рабочих дней со дня окончания проверки дает письменный ответ заявителю.

Приложение 10
к приказу МАУДО «ДПШ»
от 15.01.26 № 22-ОД

Инструкция
по резервному копированию и восстановлению данных

I. Общие положения

1. Настоящая Инструкция по резервному копированию и восстановлению данных (далее – Инструкция), хранящихся на серверах и автоматизированных рабочих местах Муниципального автономного учреждения дополнительного образования «Дворец пионеров и школьников им. Н.К. Крупской г. Челябинска» (далее – МАУДО «ДПШ») разработана в соответствии с требованиями приказа ФСТЭК России от 18.02.2013 №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

2. Настоящая Инструкция разработана с целью:

1) определения порядка резервирования данных для последующего восстановления работоспособности информационной системы (далее ИС) МАУДО «ДПШ» при полной или частичной потере информации, вызванной попытками несанкционированного доступа, сбоями или отказами аппаратного или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.);

2) определения порядка восстановления информации в случае возникновения такой необходимости;

3) упорядочения работы должностных лиц, связанной с резервным копированием и восстановлением информации.

3. В настоящем документе регламентируются действия при выполнении следующих мероприятий:

- резервное копирование;
- контроль резервного копирования;
- хранение резервных копий;
- полное или частичное восстановление данных и приложений.

4. Если резервирование предполагает выгрузку на съемные носители информации, то такие носители должны учитываться в порядке, установленном «Инструкцией ответственного за обеспечение безопасности персональных данных в информационных системах».

II. Термины и определения

5. **Автоматизированное рабочее место (АРМ)** – персональный компьютер и подключенные к нему периферийные устройства – принтер, многофункциональные устройства, сканеры и т.д.

Информация – сведения (сообщения, данные) независимо от формы их представления (Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»).

Информационная система (ИС) – система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию.

Носитель информации – любой материальный объект или среда, используемый для хранения или передачи информации.

Программное обеспечение – все или часть программ, процедур, правил и соответствующей документации системы обработки информации (ISO/IEC 2382-1:1993).

Резервное копирование – процесс создания копии данных на носителе (дисковом массиве, магнитной ленте и т. д.), предназначенном для восстановления данных в оригинальном месте их расположения в случае их повреждения или разрушения.

Система резервного копирования – совокупность программного и аппаратного обеспечения, выполняющая задачу резервного копирования информации.

III. Порядок резервного копирования

6. Резервному копированию подлежит информация следующих основных категорий:

- данные (файлы и каталоги) на файловых серверах;
- базы данных, содержащие защищаемую информацию.

7. Система резервного копирования должна обеспечивать производительность, достаточную для сохранения информации, в установленные сроки и с заданной периодичностью.

8. О выявленных попытках несанкционированного доступа к резервируемой информации, а также иных нарушениях информационной безопасности произошедших в процессе резервного копирования, должно быть немедленно сообщено ответственному за обеспечение безопасности персональных данных в информационных системах, либо ответственному за организацию обработки персональных данных МАУДО «ДПШ».

9. Для организации системы резервного копирования используются стандартные средства Windows.

10. Существуют следующие наборы резервных копий:

1) месячный набор. Записывается информация на первое число текущего месяца. Срок хранения – 1 (один) месяц.

2) недельная копия. Записывается в ночь на среду и в ночь на субботу. Срок хранения – субботняя копия – до следующей среды, вторничная копия – до субботы.

3) суточная копия. Записывается ежедневно в 12:00. Срок хранения – сутки.

11. Копии хранятся на сервере резервного копирования.

12. Для резервирования информации, хранимой непосредственно в файловых системах, используются стандартные средства Windows.

13. Для резервирования информации, хранимой в базах данных ИС МАУДО «ДПШ», в качестве промежуточного звена автоматизации используются средства конфигурирования ИС и архиваторы. В результате работы промежуточного звена автоматизации формируется каталог с резервной копией данных ИС. Посредством стандартных средств Windows формируются задания на проведение резервного копирования этого каталога.

14. При резервировании информации следует руководствоваться инструкциями, описанными в документации на систему резервного копирования ПО.

IV. Контроль результатов резервного копирования

15. Контроль результатов всех процедур резервного копирования осуществляется ответственным за обеспечение безопасности персональных данных в информационных системах.

16. На протяжении периода времени, когда система резервного копирования находится в аварийном состоянии, должно осуществляться ежедневное копирование информации, подлежащей резервированию, с использованием средств файловых систем серверов, располагающих необходимыми объемами дискового пространства для её хранения.

V. Ротация носителей резервной копии

17. Система резервного копирования должна обеспечивать возможность периодической замены (выгрузки) резервных носителей без потерь информации на них, а также обеспечивать восстановление текущей информации ИС в случае отказа любого из устройств резервного копирования. Все процедуры по загрузке, выгрузке носителей из системы резервного копирования, а также их перемещение, осуществляются ответственным за обеспечение безопасности персональных данных в информационных системах. В качестве новых носителей допускается повторно использовать те, у которых срок хранения содержащейся информации истек.

18. Носители с защищаемой информацией, которые перестали использоваться в системе резервного копирования, должны стираться (форматироваться) с использованием специального программного обеспечения, реализующим полное физическое уничтожение данных.

VI. Восстановление информации из резервной копии

19. В случае необходимости, восстановление данных из резервных копий производится на основании заявки пользователя ИС. После поступления заявки,

восстановление данных осуществляется в максимально сжатые сроки, ограниченные техническими возможностями системы, но не более 1 (одного) рабочего дня.

20. Любое восстановление информации выполняется на основании заявки пользователя ответственному за обеспечение безопасности персональных данных в информационных системах или в случае необходимости восстановления утерянной или повреждённой информации, подлежащей резервированию. В процессе восстановления резервной копии следует руководствоваться инструкциями по восстановлению информации из резервных копий, описанных в документации, на систему резервного копирования ПО.

Приложение 11
к приказу МАУДО «ДПШ»
от 19.01.26 № 22-од

Инструкция
по организации антивирусной защиты
информационной системы МАУДО «ДПШ»

I. Общие положения

1. Данная Инструкция определяет требования к организации защиты информационной системы (далее – ИС) Муниципального автономного учреждения дополнительного образования «Дворец пионеров и школьников им. Н.К. Крупской г. Челябинска» (далее – МАУДО «ДПШ») от разрушающего воздействия компьютерных вирусов и другого вредоносного программного обеспечения (далее – вредоносное ПО), устанавливает ответственность пользователей ИС, ответственного за обеспечение безопасности персональных данных в информационных системах и других должностных лиц, за выполнение указанных требований.

II. Термины и определения

2. **Антивирусная база** – это база, которая содержит уникальные данные о каждом конкретном вирусе.

Антивирусная защита – комплекс мер, направленных на предотвращение, обнаружение и обезвреживание действий вредоносного программного обеспечения при помощи антивирусных программных продуктов.

Средство антивирусной защиты – программный пакет, предназначенный для эффективной защиты, перехвата и удаления из операционной системы компьютера максимального количества вредоносных (или потенциально вредоносных) программ.

Автоматизированное рабочее место (АРМ) – персональный компьютер и подключенные к нему периферийные устройства – принтер, многофункциональные устройства, сканеры и т.д.

Информация – сведения (сообщения, данные) независимо от формы их представления (Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»).

Информационная система (ИС) – система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т.д.), которые обеспечивают и распространяют информацию.

Носитель информации – любой материальный объект или среда, используемые для хранения или передачи информации.

Программное обеспечение (ПО) – все или часть программ, процедур, правил и соответствующей документации системы обработки информации (ISO/IEC 2382-1:1993).

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (ст. 3 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»).

III. Обязанности ответственного за обеспечение безопасности персональных данных в информационных системах

3. К использованию в МАУДО «ДПШ» допускаются только сертифицированные и лицензионные средства антивирусной защиты, закупленные у разработчиков или поставщиков данных средств.

4. Установка средств антивирусного контроля на АРМ и серверах ИС МАУДО «ДПШ» осуществляется ответственным за обеспечение безопасности персональных данных в информационных системах или под его контролем, настройка параметров средств антивирусного контроля осуществляется в соответствии с руководствами по применению конкретных антивирусных средств и требованиями нормативных документов ФСТЭК РФ в области защиты информации.

5. Антивирусный контроль должен быть настроен в режиме постоянной антивирусной защиты.

6. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), хранящаяся на АРМ, передающаяся по сети, а также информация на съемных носителях. Контроль входящей информации должен осуществляться автоматически, непосредственно после её приёма. При передаче файлов, запакованных в архивы, без их распаковки, должна вручную инициироваться антивирусная проверка этих архивов.

7. Процедура обновления баз средства антивирусной защиты должна проводиться в автоматическом режиме не реже 1 (одного) раза в день на всех АРМ ИС, работающих в сети, не реже 1 (одного) раза в неделю для всех АРМ ИС, работающих автономно.

8. Устанавливаемое (изменяемое) ПО должно быть предварительно проверено ответственным за обеспечение безопасности персональных данных в информационных системах на предмет отсутствия вредоносного ПО.

9. Подключаемые к компьютеру внешние устройства и носители информации должны проверяться антивирусным ПО непосредственно после подключения.

10. Периодический контроль за состоянием антивирусной защиты (обновление антивирусной программы и антивирусных баз, а также проверка работоспособности средств антивирусной защиты) в ИС МАУДО «ДПШ» осуществляется ответственным за обеспечение безопасности персональных данных в информационных системах, пользователями ИС и всеми должностными лицами, настраивающими и сопровождающими средства антивирусной защиты в ИС МАУДО «ДПШ».

IV. Обязанности пользователя ИС

11. При возникновении подозрения на наличие вредоносного ПО (частые ошибки в работе программ, появление посторонних графических и звуковых эффектов, искажения данных, неконтролируемое пропадание файлов, появление сообщений о системных ошибках, замедление работы компьютера и т.п.) самостоятельно или вместе с ответственным за обеспечение безопасности персональных данных в информационных системах провести внеочередной антивирусный контроль своего АРМ. При самостоятельном проведении антивирусного контроля - уведомить о результатах ответственного за обеспечение безопасности персональных данных в информационных системах для определения им факта наличия или отсутствия вредоносного ПО.

12. В случае появления информационного окна средства антивирусной защиты, сигнализирующем об обнаружении вредоносного ПО:

1) приостановить обработку данных;

2) немедленно поставить в известность о факте обнаружения вредоносного ПО ответственного за обеспечение безопасности информации, владельца заражённых файлов, а также смежные структурные подразделения, использующие эти файлы в работе;

3) совместно с владельцем файлов, заражённых вредоносным ПО, провести анализ необходимости дальнейшего их использования;

4) произвести лечение или уничтожение заражённых файлов (при необходимости для выполнения требований данного пункта привлечь ответственного за обеспечение безопасности персональных данных в информационных системах).

V. Ответственность

13. Работники несут персональную ответственность за соблюдение требований настоящей Инструкции, за качество проводимых им работ по обеспечению безопасности персональных данных и за все действия, совершенные от имени их учётных записей в ИС, если с их стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учётной записи.

14. Работники при нарушении норм, регулирующих получение, обработку и защиту информации, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

15. Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе другим работникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных локальными нормативно-правовыми актами (приказами, распоряжениями) МАУДО «ДПШ», влечет наложение на работника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания,

выговора, увольнения. Работник МАУДО «ДПШ», имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба МАУДО «ДПШ» (в соответствии с п.7 ст.243 Трудового кодекса РФ).

В отдельных случаях, при разглашении персональных данных, работник, совершивший указанный проступок, несет ответственность в соответствии со ст.13.14 Кодекса об административных правонарушениях РФ.

16. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии со ст.137 Уголовного кодекса РФ.

Приложение 12
к приказу МАУДО «ДПШ»
от 19.01.26 № 22-од

Инструкция
по использованию корпоративной сети передачи данных

I. Общие правила работы

1. Работа в локальной вычислительной сети (далее – ЛВС) производится работниками МАУДО «ДПШ» с целью получения необходимой информации для выполнения возложенных на них должностных обязанностей в рамках работы в информационных системах персональных данных (далее – ИСПДн).
2. Работа в ЛВС производится с помощью базового компьютера и иных дополнительных устройств.
3. Запрос на установку базового компьютера, его настройку и установку сетевого программного обеспечения осуществляется руководителем подразделения по предварительной письменной заявке, написанной на имя директора МАУДО «ДПШ» в виде служебной записки.
4. Для идентификации пользователя ЛВС работнику выдается имя (учетная запись) и пароль. Имя и пароль необходимы для идентификации в ЛВС и получении доступа к ресурсам сети (сетевым дискам, принтерам и программам). Имя и пароль работника должны быть уникальны в сети. За уникальность и сохранность пароля отвечает пользователь. Пароль – информация конфиденциальная, конфиденциальность обеспечивается самим пользователем и средствами операционных систем.
5. Запрещается сообщать пароль другим пользователям ЛВС и работать под чужим паролем.
6. Пользователи ЛВС обязаны ознакомиться с данными правилами.

II. Технические нормы и правила

7. При нарушении нормальной работы сети и в случае обнаружения неисправности любого компьютерного и сетевого оборудования, а также при сбое или неправильной работе программного обеспечения пользователь обязан немедленно сообщить ответственному за обеспечение безопасности ИСПДн.
8. Поддержка и сопровождение установленного системного и сетевого программного обеспечения осуществляется ответственным за обеспечение безопасности ИСПДн.
9. При необходимости использования нового программного обеспечения, пользователь обязан согласовать его использование с ответственным за обеспечение безопасности ИСПДн.
10. По первому требованию технического специалиста пользователь обязан освободить компьютер для контроля или выполнения регламентных работ.
11. Все действия, связанные с установкой программного обеспечения, а также предоставлением доступа к конкретным ресурсам сети, осуществляются по предварительной письменной заявке, написанной на имя ответственного за обеспечение безопасности ИСПДн, в виде служебной записки.
12. Ответственность за работоспособность клиентского программного обеспечения рабочих станций сети подразделения несет отдел информационно-технического обеспечения.

13. Ответственный за обеспечение безопасности персональных данных в ИСПДН ведёт перечень базовых компьютеров сети организации. Каждая запись содержит следующую информацию:

- имя компьютера;
- используемая операционная система;
- модель монитора;
- ресурсы, предоставляемые другим компьютерам;
- список установленного программного обеспечения;
- должность допущенного сотрудника.

14. В ЛВС осуществляется мониторинг сетевых событий. Полученные при этом электронные журналы событий используются ответственным за обеспечение безопасности персональных данных в ИСПДн для анализа работы сети, а также могут служить доказательством неправомерных действий пользователей.

III. Права и обязанности пользователей сети

15. Пользователь, использующий носители информации, несет ответственность за антивирусную чистоту содержащихся на них данных.

16. В случае получения носителя информации из сомнительного источника пользователь обязан проверить его на «вирусы». Если у него возникли сомнения, то он вправе пригласить ответственного за обеспечение безопасности ИСПДН для повторной проверки.

17. Пользователю категорически запрещается открывать подозрительные почтовые сообщения и вложенные в них файлы.

18. Пользователь обязан немедленно прекратить работу за компьютером, и обратится к ответственному за обеспечение безопасности ИСПДн для выяснения причин и выработки мер восстановления нормального функционирования корпоративной сети в случаях:

- подозрения на заражение вирусами;
- обнаружения заражения вирусами;
- нарушением безопасности работы сети.

19. Каждый пользователь в индивидуальном порядке отвечает за понимание и правильное отношение к правилам безопасности систем, которые они используют.

20. В программах, использующие парольную защиту, пользователи обязаны выбирать качественные пароли и периодически самостоятельно менять их.

IV. Ответственность пользователей сети

21. Пользователи, нарушившие нормальное (безопасное) функционирование сети, повлекшее за собой материальный и моральный ущерб организации, должностным лицам и пользователям сети несут ответственность.

22. Ответственность пользователей сети должна определяться действующим законодательством и административными мерами.

23. Административные меры должны быть соизмеримы с объектом ответственности.

V. Пользователям запрещается

24. Самостоятельно переставлять и передвигать, а также подключать компьютерную технику в помещении (в том числе при проведении генеральных

уборок, перестановке мебели и пр.).

25. Самостоятельно производить установку, настройку, модификацию и тестирование сетевого аппаратного или программного обеспечения.

26. Передавать по сети информацию, оскорбляющую честь и достоинство других абонентов сети, содержащую призывы к насилию, разжиганию межнациональной розни, информацию в зашифрованном виде, а также передавать информацию за пределы организации, если это не входит в должностные обязанности пользователей.

27. Использовать ресурсы корпоративной сети для осуществления любого рода личной или посторонней коммерческой деятельности.

28. Предпринимать какие-либо действия прямо или косвенно направленные на нарушение нормальной работы сетевого оборудования и разрушение общих информационных ресурсов.

29. Передавать кому-либо свой пароль, работать под чужим регистрационным именем, а также осуществлять любые действия, связанные с получением паролей и регистрационных записей.

VI. Безопасность и устойчивость сети

30. Составляющие безопасности сети:

- конфиденциальность - защита от несанкционированного получения информации;
- целостность - защита от несанкционированного изменения информации;
- доступность - защита от несанкционированного удержания информации и ресурсов.

Прямое или косвенное нарушение одной из данных составляющих является нарушением безопасности сети.

31. Ответственный за обеспечение безопасности ИСПДн обязан обеспечивать и поддерживать безопасность всех компонентов ЛВС.

32. Ответственный за обеспечение безопасности ИСПДн должен обеспечивать антивирусную защиту программного обеспечения.

33. Для обеспечения устойчивости и безопасности сети ответственный за обеспечение безопасности персональных данных в ИСПДн обязан проводить регулярные регламентные работы.

Приложение 13
к приказу МАУДО «ДПШ»
от 19.01.26 № 22-ОД

Инструкция
по организации парольной защиты

I. Общие положения

1. Данная Инструкция регламентирует процессы генерации, смены и прекращения действия паролей (удаления учётных записей пользователей) в информационных системах (далее – ИС) Муниципального автономного учреждения дополнительного образования «Дворец пионеров и школьников им. Н.К. Крупской г. Челябинска» (далее – МАУДО «ДПШ»), а также контроль над действиями пользователей при работе с паролями.

2. Осуществление процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИС и контроль за действиями пользователей при работе с паролями возлагается на ответственного за обеспечение безопасности персональных данных в информационных системах.

II. Термины и определения

3. **Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

Информационная система (ИС) – система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию.

Пароль – секретная комбинация цифр, знаков, слов, или осмысленное предложение, служащие для защиты информации от несанкционированного доступа к информационным ресурсам.

Пользователь – работник, участвующий в рамках своих функциональных обязанностей в процессах обработки персональных данных.

Компрометация пароля – раскрытие, обнаружение или утеря пароля.

III. Обязанности ответственного за обеспечение безопасности персональных данных в информационных системах

4. Правила формирования паролей.

Личные пароли должны генерироваться и распределяться централизованно, либо выбираться пользователями информационной системы самостоятельно с учетом следующих требований:

1) длина пароля должна быть не менее 8 символов;

2) в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

3) пароль не должен включать в себя имя пользователя, легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, абвгд и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички

домашних животных, номера автомобилей, телефонов и другие значимые сочетаний букв и знаков, которые можно угадать, основываясь на информации о пользователе;

4) при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6-ти позициях.

5. Пользователям допускается использовать пароли, составленные из первых букв слов запоминающихся высказываний в разном регистре, смешанные в произвольном порядке со специальными символами (например, Кожзгсф7!).

6. В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на ответственного за обеспечение безопасности персональных данных в информационных системах.

7. Порядок смены личных паролей.

7.1. Смена паролей должна проводиться регулярно, не реже одного раза в 3 месяца.

7.2. В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т.п.) должно производиться немедленное удаление его учётной записи сразу после окончания последнего сеанса работы данного пользователя с системой.

7.3. Срочная (внеплановая) полная смена паролей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) ответственных за обеспечение безопасности персональных данных в информационных системах, администраторов информационной системы и других работников, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.

7.4. Ответственный за обеспечение безопасности персональных данных в информационных системах ведёт «Журнал учёта работ в информационных системах», в котором он отмечает факт смены паролей пользователей.

7.5. Временный пароль, заданный ответственным за обеспечение безопасности персональных данных в информационных системах при регистрации нового пользователя, должен действовать в течение ограниченного срока времени. Пользователь должен изменить временный пароль при первом входе в систему.

8. В случае утери или компрометации (разглашения, утраты) или подозрения в компрометации пароля пользователя должна быть немедленно проведена внеплановая процедура смены пароля.

IV. Обязанности пользователя ИС

9. Правила формирования паролей.

Личные пароли должны генерироваться и распределяться централизованно, либо выбираться пользователями информационной системы самостоятельно с учетом следующих требований:

1) длина пароля должна быть не менее 6 символов;

2) в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

3) пароль не должен включать в себя имя пользователя, легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, абвгд и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички

домашних животных, номера автомобилей, телефонов и другие значимые сочетаний букв и знаков, которые можно угадать, основываясь на информации о пользователе;

4) при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6-ти позициях.

10. Работникам допускается использовать пароли, составленные из первых букв слов запоминающихся высказываний в разном регистре, смешанные в произвольном порядке со специальными символами (например, Кожзгсф7!).

11. Для обеспечения возможности использования имён и паролей некоторых работников в их отсутствие (например, в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п.), работники обязаны сразу же после установки своих паролей передавать их на хранение вместе с именами своих учетных записей ответственному за обеспечение безопасности персональных данных в информационных системах в запечатанном конверте или опечатанном пенале.

12. При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его подсматривания посторонними лицами (человек за спиной, наблюдение человеком за движением пальцев в прямой видимости или в отраженном свете) и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т.п.).

13. Смена паролей должна проводиться регулярно, не реже одного раза в 3 месяца, самостоятельно каждым пользователем.

14. Временный пароль, заданный ответственным за обеспечение безопасности персональных данных в информационных системах при регистрации нового пользователя, должен действовать в течение ограниченного срока времени. Пользователь должен изменить временный пароль при первом входе в систему.

15. Хранение пароля.

15.1. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке, мобильном телефоне и любых других предметах и носителях информации.

15.2. Запрещается сообщать свой пароль полностью или частично другим пользователям, запрещается спрашивать или подсматривать пароль других пользователей.

15.3. Запрещается регистрировать других пользователей в ИС со своим личным паролем, запрещается входить в ИС под учётной записью и паролем другого пользователя.

16. В случае утери или компрометации (разглашения, утраты) или подозрения в компрометации пароля пользователь должен немедленно обратиться к ответственному за обеспечение безопасности персональных данных в информационных системах с целью смены личного пароля.

V. Ответственность

17. Работники несут персональную ответственность за соблюдение требований настоящей Инструкции, за качество проводимых ими работ по обеспечению безопасности информации и за все действия, совершенные от имени их учётных записей в ИС, если с их стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учётной записи.

18. Работники при нарушении норм, регулирующих получение, обработку и защиту информации, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

19. Разглашение информации (передача их посторонним лицам, в том числе другим работникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных локальными нормативно-правовыми актами (приказами, распоряжениями) МАУДО «ДПШ», влечет наложение на работника, имеющего доступ к защищаемой информации, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Работник МАУДО «ДПШ», имеющий доступ к информации и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба МАУДО «ДПШ» (в соответствии с п.7 ст.243 Трудового кодекса РФ).

В отдельных случаях, при разглашении персональных данных, работник, совершивший указанный проступок, несет ответственность в соответствии со статьей 13.14 Кодекса об административных правонарушениях РФ.

20. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии со ст. 137 Уголовного кодекса РФ.

Приложение 14
к приказу МАУДО «ДПШ»
от 19.01.26 № 22-08

Инструкция
ответственного за организацию обработки персональных данных

I. Общие положения

1. Данная Инструкция определяет основные обязанности и права ответственного за организацию обработки персональных данных Муниципального автономного учреждения дополнительного образования «Дворец пионеров и школьников им. Н.К. Крупской г. Челябинска» (далее - МАУДО «ДПШ»).

2. Ответственный за организацию обработки персональных данных является штатным работником МАУДО «ДПШ» и назначается приказом директора.

3. Решение вопросов организации защиты персональных данных в МАУДО «ДПШ» входит в прямые служебные обязанности ответственного за организацию обработки персональных данных.

4. Ответственный за организацию обработки персональных данных обладает правами доступа к любым носителям персональных данных МАУДО «ДПШ».

II. Термины и определения

5. **Блокирование персональных данных** – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных) (ст.3 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»).

Доступ к информации – возможность получения информации и её использования (ст.2 Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и защите информации»).

Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств (ст.3 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»).

Несанкционированный доступ (НСД) – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путём изменения (повышения, фальсификации) своих прав доступа.

Носитель информации - любой материальный объект или среда, используемый для хранения или передачи информации.

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных (ст.3 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»).

Пользователь – работник, участвующий в рамках своих функциональных обязанностей в процессах обработки персональных данных.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (ст.3 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»).

Средство защиты информации (СЗИ) – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

III. Должностные обязанности

6. Ответственный за организацию обработки персональных данных обязан осуществлять внутренний контроль за исполнением сотрудниками МАУДО «ДПШ» требований законодательства Российской Федерации и положений локальных нормативных актов МАУДО «ДПШ» при обработке персональных данных, доводить до сведения работников учреждения нормы законодательства и внутренних локальных актов по работе с персональными данными, в том числе:

1) знать перечень и условия обработки персональных данных в МАУДО «ДПШ»;

2) знать и предоставлять изменения на утверждение директору к списку лиц, доступ которых к персональным данным необходим для выполнения ими своих служебных (трудовых) обязанностей;

3) участвовать в определении полномочий пользователей ИСПДн (оформлении разрешительной системы доступа), минимально необходимых им для выполнения служебных (трудовых) обязанностей;

4) осуществлять учёт документов, содержащих персональные данные, их уничтожение, либо контроль процедуры их уничтожения;

5) блокировать доступ к персональным данным при обнаружении нарушений порядка их обработки;

6) реагировать на попытки несанкционированного доступа к информации в установленном гл. IV настоящей Инструкции порядке;

7) контролировать осуществление мероприятий по установке и настройке средств защиты информации;

8) производить периодический контроль за соблюдением режима безопасности помещений, в которых размещена информационная система, путем:

- контроля расположения мониторов для исключения визуального доступа к нему возможному внешнему нарушителю;

- контроля исключения визуального доступа при обработке персональных данных.

9) поддерживать в актуальном состоянии локальные документы, направленные на обеспечение защиты персональных данных;

10) при приеме/увольнении работников актуализировать документ «Список лиц, доступ которых к защищаемой информации необходим для выполнения служебных (трудовых) обязанностей»;

11) организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов;

12) по указанию руководства своевременно и точно отражать изменения в локальных нормативно-правовых актах по управлению средствами защиты информации в ИСПДн и правилам обработки персональных данных;

13) в установленные законодательством сроки регистрировать и отвечать на поступающие запросы и обращения субъектов ПДн или их законных представителей;

14) проводить занятия и инструктажи с работниками и руководителями структурных подразделений о порядке работы с персональными данными и изучение руководящих документов в области обеспечения безопасности персональных данных;

15) проводить разбирательства и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с документами, содержащими персональные данные, или по другим нарушениям, которые могут привести к снижению уровня защищённости персональных данных;

16) контролировать соблюдение работниками локальных документов, регламентирующих порядок работы с программными, техническими средствами ИСПДн и персональными данными;

17) вносить свои предложения по совершенствованию мер защиты персональных данных в ИСПДн, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня защищённости персональных данных;

18) организовать учет обращений субъектов персональных данных, контролировать заполнение «Журнала учета обращений субъектов персональных данных»;

19) представлять интересы МАУДО «ДПШ» при проверках надзорных органов в сфере обработки персональных данных;

20) знать законодательство РФ о персональных данных, следить за его изменениями;

21) выполнять иные мероприятия, требуемые нормативными документами по защите персональных данных.

IV. Действия при обнаружении попыток несанкционированного доступа

7. К попыткам несанкционированного доступа относятся:

- сеансы работы с персональными данными незарегистрированных пользователей, или пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истёк, или превышающих свои полномочия по доступу к данным;
- действия третьего лица, пытающегося получить доступ (или уже получившего доступ) к ИСПДн, при использовании учётной записи администратора или другого пользователя ИСПДн, методом подбора пароля, использования пароля, разглашённого владельцем учётной записи или любым другим методом.

8. При выявлении факта несанкционированного доступа ответственный за организацию обработки персональных данных обязан:

1) прекратить несанкционированный доступ к персональным данным;

2) доложить директору МАУДО «ДПШ» служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;

3) известить руководителя структурного подразделения, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка несанкционированного доступа, о факте несанкционированного доступа;

4) известить ответственного за обеспечение безопасности персональных данных в информационных системах о факте несанкционированного доступа.

V. Права

9. Ответственный за организацию обработки персональных данных имеет право:

1) доступа ко всем персональным данным субъектов персональных данных, обрабатываемых в МАУДО «ДПШ»;

2) требовать от работников выполнения норм законодательства Российской Федерации о персональных данных, внутренних локальных нормативно-правовых актов в части работы с персональными данными;

3) блокировать доступ к персональным данным любых пользователей, если это необходимо для предотвращения нарушения режима защиты персональных данных;

4) проводить служебные расследования и опрашивать пользователей по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с техническими и программными средствами ИСПДн, в том числе со средствами защиты информации, или по другим нарушениям, которые могут привести к снижению уровня защищённости персональных данных.

VI. Ответственность

10. Ответственный за организацию обработки персональных данных несёт персональную ответственность за соблюдение требований настоящей Инструкции, за качество проводимых им работ по обеспечению безопасности персональных данных и за все действия, совершенные от имени его учётной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учётной записи.

11. Ответственный за организацию обработки персональных данных при нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несёт дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

12. Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе другим работникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных локальными нормативно-правовыми актами (приказами, распоряжениями) МАУДО «ДПШ», влечет наложение на работника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Работник МАУДО «ДПШ», имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба МАУДО «ДПШ» (в соответствии с п.7 ст.243 Трудового кодекса РФ).

В отдельных случаях, при разглашении персональных данных, работник, совершивший указанный проступок, несет ответственность в соответствии со ст.13.11, 13.14 Кодекса об административных правонарушениях РФ.

13. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии со ст.137 Уголовного кодекса РФ.

Приложение 15
к приказу МАУДО «ДПШ»
от 19.01.26 №22-д

Инструкция
ответственного за обеспечение безопасности персональных данных в информационных системах

I. Общие положения

1. Данная Инструкция определяет основные обязанности и права ответственного за обеспечение безопасности персональных данных в информационных системах, в том числе персональных данных, Муниципального автономного учреждения дополнительного образования «Дворец пионеров и школьников им. Н.К. Крупской г. Челябинска» (далее - МАУДО «ДПШ»).

2. Ответственный за обеспечение безопасности персональных данных в информационных системах назначается приказом директора.

3. Решение вопросов обеспечения информационной безопасности входит в прямые служебные обязанности ответственного за обеспечение безопасности персональных данных в информационных системах.

4. Ответственный за обеспечение безопасности персональных данных в информационных системах обладает правами доступа к любым программным и аппаратным ресурсам информационной системы (далее - ИС) МАУДО «ДПШ».

5. Целью защиты информации является:

5.1. Предотвращение утечки, хищения, утраты, подделки информации, а также неправомерных действий по уничтожению, модификации, искажению, несанкционированному копированию, блокированию информации, предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы обеспечения правового режима документированной информации как объекта собственности.

5.2. Защита конституционных прав граждан на сохранение личной тайны и конфиденциальности информации, имеющейся в ИС МАУДО «ДПШ».

5.3. Сохранение конфиденциальности информации в соответствии с законодательством Российской Федерации.

5.4. Обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

6. Основными видами угроз безопасности защищаемой информации являются:

- противоправные действия третьих лиц;
- ошибочные действия пользователей ИС;
- отказы и сбои технических средств ИС, приводящие к её модификации, блокированию, уничтожению или несанкционированному копированию, а также нарушению правил эксплуатации ЭВМ и сетевого оборудования.

II. Термины и определения

7. **Автоматизированное рабочее место (АРМ)** – персональный компьютер и подключенные к нему периферийные устройства – принтер, многофункциональные устройства, сканеры и т.д.

Антивирусная защита – комплекс мер, направленных на предотвращение, обнаружение и обезвреживание действий вредоносного ПО при помощи антивирусных программных продуктов.

База данных – это информация, упорядоченная в виде набора элементов, записей одинаковой структуры.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и / или воздействия на защищаемую информацию или ресурсы информационной системы.

Дистрибутив программного обеспечения – это файл или файлы, предназначенные для установки программного обеспечения.

Доступ к информации – возможность получения информации и её использования (ст.2 Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и защите информации»).

Защита информации – деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на информацию, то есть процесс, направленный на достижение информационной безопасности.

Конфиденциальная информация – документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации (ФСТЭК. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) Москва 2001).

Несанкционированный доступ (НСД) – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путём изменения (повышения, фальсификации) своих прав доступа.

Носитель информации – любой материальный объект или среда, используемый для хранения или передачи информации.

Обработка информации – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с информацией, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение информации.

Пользователь – работник, участвующий в рамках своих функциональных обязанностей в процессах обработки информации.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (ст.3 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»).

Резервное копирование – процесс создания копии данных на носителе (дисковом массиве, магнитной ленте и т. д.), предназначенном для восстановления данных в оригинальном месте их расположения в случае их повреждения или разрушения.

Средство защиты информации (СЗИ) – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Угрозы безопасности защищаемой информации (УБЗИ) – совокупность условий и факторов, создающих опасность несанкционированного, в том числе

случайного, доступа к защищаемой информации, результатом которого может стать уничтожение, изменение, блокирование, копирование, предоставление, распространение информации, а также иные неправомерные действия при их обработке в информационной системе.

Уничтожение информации – действия, в результате которых становится невозможным восстановить содержание защищаемой информации в информационной системе и (или) в результате которых уничтожаются материальные носители защищаемой информации.

Утечка защищаемой информации – неконтролируемое распространение информации от ее носителя.

III. Общие обязанности

8. Ответственный за обеспечение безопасности персональных данных в информационных системах обязан:

1) знать перечень сведений, составляющих защищаемую информацию и условия ее обработки в МАУДО «ДПШ»;

2) знать перечень установленных в отделах МАУДО «ДПШ» технических средств, в том числе съёмных носителей, конфигурацию ИС и перечень задач, решаемых с её использованием;

3) определять полномочия пользователей ИС (оформление разрешительной системы доступа), минимально необходимых им для выполнения служебных (трудовых) обязанностей;

4) осуществлять учёт съемных носителей информации, их уничтожение, либо контроль процедуры их уничтожения, вести «Журнал учета съемных носителей информации»;

5) осуществлять оперативный контроль за работой пользователей защищённых АРМ и адекватно реагировать на возникающие нештатные ситуации, фиксировать их в «Журнале учета работ в информационных системах»;

6) периодически проверять актуальность сертификатов соответствия используемых средств защиты информации в информационных системах;

7) блокировать доступ к защищаемой информации при обнаружении нарушений порядка их обработки;

8) реагировать на попытки несанкционированного доступа к информации в установленном гл. VIII настоящей Инструкции порядке;

9) устанавливать и осуществлять настройку средств защиты информации в рамках компетенции;

10) по мере необходимости вносить изменения в конфигурацию технических средств ИС, отражать соответствующие изменения в перечне АРМ информационной системы;

11) осуществлять непосредственное управление и контроль режимов работы функционирования применяемых в ИС средств защиты информации, осуществлять проверку правильности их настройки (выборочное тестирование);

12) периодически контролировать целостность печатей (пломб, наклеек) технических средств, используемых для обработки защищаемой информации;

13) проводить работу по выявлению возможных каналов утечки информации, изучать текущие тенденции в области защиты персональных данных;

14) проводить разбирательства и составление заключений по фактам несоблюдения условий хранения носителей информации, нарушения правил работы с

техническими и программными средствами ИС, в том числе со средствами защиты информации, или по другим нарушениям, которые могут привести к снижению степени защищённости;

15) предоставлять доступ к ИС новым пользователям, предоставлять им возможность задать личный пароль, соответствующий требованиям Инструкции по организации парольной защиты;

16) производить мероприятия по внеплановой смене личных паролей;

17) вносить плановые и внеплановые изменения в учётную запись пользователей ИС, в том числе по требованию руководителя структурного подразделения и в случае увольнения работника;

18) осуществлять периодическое резервное копирование баз данных и сопутствующей защищаемой информации, а также осуществлять внеплановое создание резервных копий по требованию пользователей ИС и в иных случаях, когда это необходимо для обеспечения сохранности персональных данных;

19) осуществлять восстановление информации из резервных копий по требованию пользователей ИС и в иных случаях, когда это необходимо для восстановления утраченных сведений;

20) хранить дистрибутивы программного обеспечения, установленного в ИС, в том числе дистрибутивы средств защиты информации, в месте, исключающем несанкционированный доступ к ним третьих лиц;

21) вносить свои предложения по совершенствованию мер защиты информации в ИС, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению степени защищённости;

22) заниматься обслуживанием установленных средств криптографической защиты информации (в том числе персональных данных);

23) знать законодательство РФ о защите информации, следить за его изменениями;

24) выполнять иные мероприятия, требуемые техническими и программными средствами ИС для поддержания их функционирования;

25) при использовании в информационных системах технологий беспроводного доступа, разграничивать доступ к беспроводной сети, контролировать предоставление доступа к беспроводной сети только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (при наличии сертифицированных средств защиты информации);

26) контролировать запрет обработки защищаемой информации с использованием технологии беспроводного доступа к сети (при отсутствии сертифицированных средств защиты информации).

IV. Порядок работы со съёмными носителями

9. Под съемными носителями (далее – носители) в настоящей Инструкции понимаются следующие носители информации:

- USB-флеш-накопитель;
- оптические диски (CD, DVD) однократной и многократной записи;
- электронные накопители информации (в т.ч. съемные жесткие диски).

10. Носители, содержащие защищаемую информацию, подлежат обязательному учету ответственным за обеспечение безопасности персональных данных в информационных системах в Журнале учета съемных носителей информации.

11. Носители, содержащие защищаемую информацию, должны иметь специальную маркировку. Тип маркировки выбирается ответственным за обеспечение безопасности персональных данных в информационных системах.

12. При поступлении нового носителя, который будет использоваться для хранения или передачи защищаемой информации, ответственный за обеспечение безопасности персональных данных в информационных системах регистрирует его в Журнале учета съемных носителей информации.

13. Учет выдачи носителей ведётся в Журнале учета съемных носителей информации, в котором указывается маркировка носителя, дата, время, фамилия, имя и отчество должностного лица, получившего материальный носитель, его подпись.

14. В случае возврата должностным лицом носителя в Журнале учета съемных носителей информации ответственным за обеспечение безопасности персональных данных в информационных системах проставляется отметка о возврате с указанием даты, времени возврата, личных подписей передающей и принимающей стороны.

V. Разграничение доступа пользователей к информационным ресурсам и средствам защиты информации

15. Защита от несанкционированного доступа осуществляется:

1) идентификацией и проверкой подлинности пользователей ИС при доступе к информационным ресурсам МАУДО «ДПШ»;

2) разграничением доступа к обрабатываемым базам данных. Пользователь ИС имеет доступ только к тем информационным ресурсам, которые разрешены для него. Для осуществления доступа к информационным ресурсам, ответственный за обеспечение безопасности персональных данных в информационных системах назначает конкретному пользователю ИС идентифицирующее имя пользователя и персональный пароль доступа.

16. Ответственный за обеспечение безопасности персональных данных в информационных системах должен осуществлять мероприятия по обеспечению защиты информационных ресурсов МАУДО «ДПШ» от несанкционированного доступа и непреднамеренных изменений и разрушений, а также иметь в наличии средства восстановления, резервные копии, предусматривающие процедуру восстановления свойств информационных ресурсов после сбоев и отказов оборудования.

VI. Действия при обнаружении попыток несанкционированного доступа

17. К попыткам несанкционированного доступа относятся:

- сеансы работы с ИС незарегистрированных пользователей, или пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истёк, или превышающих свои полномочия по доступу к данным;

- действия третьего лица, пытающегося получить доступ (или уже получившего доступ) к ИС, при использовании учётной записи администратора или другого пользователя ИС, методом подбора пароля, использования пароля, разглашённого владельцем учётной записи или любым другим методом.

18. При выявлении факта несанкционированного доступа ответственный за обеспечение безопасности персональных данных в информационных системах обязан:

1) прекратить несанкционированный доступ к ИС;

2) доложить директору МАУДО «ДПШ» служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;

3) известить руководителя структурного подразделения, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка несанкционированного доступа, о факте несанкционированного доступа.

VII. Права

19. Ответственный за обеспечение безопасности персональных данных в информационных системах, имеет право:

1) требовать от пользователей ИС выполнения инструкций в части работы с программными, аппаратными средствами ИС и защищаемой информацией;

2) блокировать доступ к защищаемой информации любых пользователей, если это необходимо для предотвращения нарушения режима защиты информации;

3) проводить внеплановые антивирусные проверки при возникновении угрозы появления вредоносных программ;

4) производить периодические попытки взлома паролей пользователей в целях тестирования системы контроля доступа на наличие уязвимостей. В случае успешной попытки – вправе требовать у пользователя изменения пароля;

5) проводить служебные расследования и опрашивать пользователей по фактам несоблюдения условий хранения носителей информации, нарушения правил работы с техническими и программными средствами ИС, в том числе со средствами защиты информации, или по другим нарушениям, которые могут привести к снижению степени защищённости.

VIII. Ответственность

20. Ответственный за обеспечение безопасности персональных данных в информационных системах несёт персональную ответственность за соблюдение требований настоящей Инструкции, за средства защиты информации, применяемые в ИС МАУДО «ДПШ», за качество проводимых им работ по обеспечению безопасности защищаемой информации и за все действия, совершенные от имени его учётной записи в ИС, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учётной записи.

21. Ответственный за обеспечение безопасности персональных данных в информационных системах при нарушении норм, регулирующих получение, обработку и защиту информации, несёт дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

22. Разглашение защищаемой информации (передача ее посторонним лицам, в том числе другим работникам, не имеющим к ней допуск), ее публичное раскрытие, утрата документов и иных носителей, содержащих защищаемую информацию субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных локальными нормативно-правовыми актами (приказами, распоряжениями) МАУДО «ДПШ», влечет наложение на работника, имеющего доступ к защищаемой информации, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Работник МАУДО «ДПШ», имеющий доступ к защищаемой информации субъекта и совершивший указанный дисциплинарный проступок, несет

полную материальную ответственность в случае причинения его действиями ущерба МАУДО «ДПШ» (в соответствии с п.7 ст.243 Трудового кодекса РФ).

В отдельных случаях, при разглашении защищаемой информации, работник, совершивший указанный проступок, несет ответственность в соответствии со ст.13.11, 13.14 Кодекса об административных правонарушениях РФ.

23. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии со ст.137 Уголовного кодекса РФ.

ФОРМА

Приложение 16
к приказу МАУДО «ДПШ»
от 19.01.26 № 22-од

ЖУРНАЛ

учета обращений субъектов персональных данных Муниципального автономного учреждения дополнительного образования «Дворец пионеров и школьников им. Н.К. Крупской г. Челябинска»

Начат:	
Окончен:	
Количество листов:	
Срок хранения:	**5 лет**

Порядок заполнения Журнала учета обращений субъектов персональных данных

1. В графу «Дата обращения» вносится дата поступления обращения;
2. В графу «Ф.И.О. обратившегося» вносятся фамилия и инициалы автора обращения;
3. В графу «ФИО субъекта персональных данных» вносятся фамилия и инициалы гражданина-субъекта персональных данных;
4. В графу «Адрес субъекта персональных данных» вносится адрес местожительства гражданина-субъекта персональных данных;
5. В графу «Вид обращения и его краткое содержание» вносится информация о виде обращения (о наличии и на ознакомление с ПДн/на уточнение ПДн/на уничтожение ПДн/с отзывом согласия на обработку ПДн) и его краткое содержание;
6. В графу «Принятое решение» вносится информация о результатах рассмотрения обращения;
7. В графу «Ф.И.О., должность принявшего запрос» вносятся фамилия, инициалы и должность работника, принявшего запрос.

№ п/п	Дата обращения	Ф.И.О. обратившегося	ФИО субъекта персональных данных	Адрес субъекта персональных данных

ФОРМА

Приложение 17
к приказу МАУДО «ДПШ»
от 19.01.26 № 22-09

ЖУРНАЛ

учета работ в информационных системах Муниципального автономного учреждения дополнительного образования «Дворец пионеров и школьников им. Н.К. Крупской г. Челябинска»

Начат:	
Окончен:	
Количество листов:	
Срок хранения:	**5 лет**

Порядок заполнения Журнала учета работ в информационных системах

1. В графу «Дата» вносится дата проведения работ в информационной системе персональных данных.
2. В графу «Наименование работ» вносится перечень работ, выполненных в информационной системе персональных данных.
3. В графу «Ф.И.О. исполнителя работ» вносятся фамилия и инициалы работника, производившего работы в информационной системе персональных данных.
4. В графу «ИСПДн» вносится название информационной системы персональных данных, в которой проводились работы (название ИСПДн можно уточнить в перечне АРМ или техническом паспорте).
5. В графу «Подпись» ставится личная подпись работника, подтверждающая факт выполнения заявленных работ.

№ п/п	Дата	Наименование работ	Ф.И.О. исполнителя работ	Информационная система	Подпись

ФОРМА

Приложение 18
к приказу МАУДО «ДПШ»
от 19.01.26 № 22-07

ЖУРНАЛ

учёта съемных носителей информации Муниципального автономного учреждения дополнительного образования «Дворец пионеров и школьников им. Н.К. Крупской г. Челябинска»

Начат:	
Окончен:	
Количество листов:	
Срок хранения:	**5 лет**

Порядок заполнения Журнала учета съемных носителей информации

1. В графу «Регистрационный (учётный) номер или маркировка носителя» вносится номер, под которым зарегистрирован данный носитель (обычно написан на самом носителе). Например, ИН-000002.
2. В графу «Тип носителя и его ёмкость» вносится вид носителя (USB-flash (флэшка), дискета, CD-диск и т.д.), размер его памяти.
3. В графу «Дата поступления» вносится дата, когда данный носитель был получен (куплен) и поставлен на учет в организации.
4. В графу «Отметка о получении» вносятся фамилия и инициалы работника, который получил данный носитель, дата, когда данный работник получил носитель, личная подпись работника.
5. В графу «Отметка об обратном приёме» вносятся фамилия и инициалы работника, который вернул данный носитель, дата, когда данный работник вернул носитель, личная подпись работника.
6. Графа «Дата и номер акта об уничтожении» заполняется в том случае, если носитель был уничтожен. В эту графу вносятся дата и номер составленного Акта об уничтожении.
7.

№ п/п	Регистрационный (учётный) номер или маркировка носителя	Тип носителя и его ёмкость	Дата поступления	Отметка о получении (Ф.И.О., подпись, дата)	Отметка об обратном приёме (Ф.И.О., подпись, дата)	Место хранения	Дата и номер акта об уничтожении	Примечание
1	2	3	4	5	6	7	8	9

ФОРМА

Приложение 19
к приказу МАУДО «ДПШ»
от 19.01.26 № 22-ОД

ЖУРНАЛ

учёта ключей от сейфов и помещений Муниципального автономного учреждения дополнительного образования «Дворец пионеров и школьников им. Н.К. Крупской г. Челябинска»

Начат:	
Окончен:	
Количество листов:	
Срок хранения:	**5 лет**

Порядок заполнения Журнала учета ключей от сейфов и помещений

1. В графу «Номер или маркировка сейфа, помещения» вносится номер, под которым зарегистрирован данный сейф или помещение (обычно написан на самом сейфе, номер кабинета). Например, ИН-000054, кабинет 4;
2. В графу «Дата и время выдачи ключа» вносятся дата и время, когда был выдан ключ;
3. В графу «Отметка о выдаче (Ф.И.О., подпись)» вносятся фамилия, инициалы и подпись работника, который выдает данный ключ;
4. В графу «Отметка о получении (Ф.И.О., подпись)» вносятся фамилия, инициалы и подпись работника, который получает ключ;
5. В графу «Дата и время обратного приёма ключа» вносятся дата и время, когда был возвращен ключ;
6. В графу «Отметка об обратном получении (Ф.И.О., подпись)» вносятся фамилия, инициалы и подпись работника, который получает обратно данный ключ;
7. В графу «Отметка о возврате (Ф.И.О., подпись)» вносятся фамилия, инициалы и подпись работника, который возвращает данный ключ.

№ п/п	Номер или маркировка сейфа, помещения	Дата и время выдачи ключа	Отметка о выдаче (Ф.И.О., подпись)	Отметка о получении (Ф.И.О., подпись)	Дата и время обратного приёма ключа	Отметка об обратном получении (Ф.И.О., подпись)	Отметка о возврате (Ф.И.О., подпись)	Примечание
1	2	3	4	5	6	7	8	9

ФОРМА

Приложение 20
к приказу МАУДО «ДПШ»
от 19.01.26 № 22-од

Акт
уничтожения персональных данных субъектов на электронных носителях персональных данных МАУДО «ДПШ»

Составлен комиссией:

Роль	ФИО	Должность
Председатель		
Члены комиссии		

На основании достижения цели обработки персональных данных, в соответствии с требованиями Федерального закона Российской Федерации от 27 июля 2006 г. №152-ФЗ «О персональных данных» по решению комиссии, подлежат уничтожению следующие носители, содержащие персональные данные:

№ п/п	Носитель, содержащий персональные данные	Место хранения	Примечание

Указанные персональные данные уничтожены с электронных носителей путем_____.
(стирание с помощью средств гарантированного удаления информации, уничтожения носителя и т.п.)

Председатель:

_____ _____

Члены комиссии:

_____ _____

_____ _____

_____ _____

ФОРМА

Приложение 21
к приказу МАУДО «ДПШ»
от 19.01.26 № 22-8

Акт
уничтожения носителей персональных данных
субъекта(ов) персональных данных МАУДО «ДПШ»

Составлен комиссией:

Роль	**ФИО**	**Должность**
Председатель		
Члены комиссии		

На основании достижения цели обработки персональных данных, в соответствии с требованиями Федерального закона Российской Федерации от 27 июля 2006 г. №152-ФЗ «О персональных данных» по решению комиссии, подлежат уничтожению следующие носители, содержащие персональные данные:

№ п/п	**Носитель, содержащий персональные данные**	**Место хранения**	**Примечание**

Указанные носители персональных данных уничтожены путем_____.
(механического уничтожения, сжигания и т.п.)

Председатель:

_____ _____

Члены комиссии:

_____ _____
_____ _____
_____ _____

Приложение 22
к приказу МАУДО «ДПШ»
от 19.01.26 № 22-08

Обязательство
о неразглашении информации ограниченного доступа

Я,_____,
(Ф.И.О. работника)

в качестве работника Муниципального автономного учреждения дополнительного образования «Дворец пионеров и школьников им. Н.К. Крупской г. Челябинска» (далее - МАУДО «ДПШ») в период трудовых отношений с данным учреждением и в течение 3 (трех) лет после их окончания обязуюсь:

1) не разглашать сведения, составляющие информацию ограниченного доступа (доступ к которой ограничивается в соответствии с законодательством РФ) МАУДО «ДПШ», которые мне будут доверены или станут известны в процессе трудовой деятельности;

2) не передавать третьим лицам и не раскрывать публично сведения, составляющие информацию ограниченного доступа МАУДО «ДПШ»;

3) выполнять требования приказов, инструкций и положений по обеспечению сохранности информации ограниченного доступа МАУДО «ДПШ»;

4) в случае попытки посторонних лиц получить от меня сведения об информации ограниченного доступа МАУДО «ДПШ» сообщить об этом факте руководству;

5) сохранять информацию ограниченного доступа тех учреждений (организаций), с которыми у МАУДО «ДПШ» имелись и (или) имеются деловые отношения;

6) не использовать знание информации ограниченного доступа МАУДО «ДПШ» для занятий любой деятельностью, которая может нанести ущерб МАУДО «ДПШ», за исключением случаев, установленных законодательством РФ;

7) в случае моего увольнения, прекратить обработку защищаемой информации, ставшей мне известной в связи с исполнением должностных обязанностей, все носители информации ограниченного доступа МАУДО «ДПШ» (рукописи, черновики, машинные носители, распечатки на принтерах, изделия и пр.), которые находились в моем распоряжении в связи с выполнением мною служебных обязанностей во время работы в МАУДО «ДПШ», передать непосредственному руководителю;

8) об утрате или недостаче носителей информации ограниченного доступа, ключей, специальных пропусков, удостоверений от режимных помещений, хранилищ, сейфов, архивов, личных печатей, которые могут привести к разглашению информации ограниченного доступа, а также о причинах и условиях возможной утечки сведений немедленно сообщать директору МАУДО «ДПШ».

Я предупрежден(а), что в случае невыполнения любого из вышеуказанных пунктов настоящего Обязательства, ко мне могут быть применены меры дисциплинарного взыскания в соответствии с трудовым законодательством РФ, вплоть до увольнения из МАУДО «ДПШ».

Мне известно, что нарушение требований по обеспечению сохранности информации ограниченного доступа МАУДО «ДПШ» может повлечь уголовную, административную, гражданско-правовую или иную ответственность в соответствии с законодательством Российской Федерации, в виде лишения свободы, денежного штрафа, обязанности по возмещению ущерба МАУДО «ДПШ» и других наказаний.

«___»_____20___г. _____/_____
(дата) (подпись) (И.О. Фамилия)

Приложение 23
к приказу МАУДО «ДПШ»
от 19.01.26 № 22-ос

Согласие на обработку персональных данных при зачислении на обучение

Я, _____,
фамилия, имя, отчество родителя (законного представителя) несовершеннолетнего субъекта персональных данных

паспорт _____ выдан _____ «__» _____г.,
серия, номер кем выдан дата выдачи

проживающий по адресу _____,
являясь родителем (законным представителем) субъекта персональных данных

_____,
фамилия, имя, отчество несовершеннолетнего субъекта персональных данных

на основании _____,
(реквизиты документа, подтверждающего полномочия законного представителя)

проживающего по адресу_____,
свободно, своей волей и в своем интересе даю конкретное, информированное и сознательное согласие Муниципальному автономному учреждению дополнительного образования «Дворец пионеров и школьников им. Н.К. Крупской г. Челябинска», расположенному по адресу: 454080, Челябинская область, г.Челябинск, Свердловский пр., 59 (далее — Оператор), на обработку персональных данных субъектов (несовершеннолетнего ребенка и его родителя (законного представителя)) на следующих условиях:

1. Согласие дается мною в целях: оформления документов на прием в МАУДО «ДПШ», осуществления образовательного процесса, психолого-педагогическое сопровождение (в т.ч. психологическую диагностику, консультирование родителей (по индивидуальному обращению)), составления отчетности о работе МАУДО «ДПШ», участия в мероприятиях различных уровней (отправка заявки и иных документов для участия), публикации результатов освоения дополнительных общеобразовательных программ, результатов участия в мероприятиях (в том числе на официальном сайте МАУДО «ДПШ»).

2. Настоящее согласие дается на осуществление следующих действий в отношении персональных данных субъектов, которые необходимы для достижения указанных выше целей, совершаемых с использованием средств автоматизации и без использования таких средств, включая без ограничения: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных, а также любых иных действий с учетом действующего законодательства РФ.

3. Перечень персональных данных несовершеннолетнего субъекта, передаваемых Оператору на обработку: фамилия, имя, отчество; пол; дата рождения; данные документа, удостоверяющего личность (вид, серия, номер, дата выдачи, наименование органа, выдавшего документ); данные о месте жительства; данные о

местах обучения; состояние здоровья; фотография; сведения о посещаемости занятий; данные ИНН, данные страхового пенсионного свидетельства; контактный телефон; сведения о родителях (законных представителях) субъекта.

4. Перечень персональных данных родителя (законного представителя) несовершеннолетнего субъекта, передаваемых Оператору на обработку: фамилия, имя, отчество; данные документа, удостоверяющего личность (вид, серия, номер, дата выдачи, наименование органа, выдавшего документ); данные о месте жительства; контактный телефон; место работы, должность, социальное положение семьи.

5. Оператор имеет право передавать персональные данные несовершеннолетнего субъекта в Комитет по делам образования города Челябинска и иные организации для достижения указанных выше целей в случаях, установленных документами вышестоящих органов и законодательством РФ.

6. Настоящее согласие дается до достижения цели обработки персональных данных либо утраты правовых оснований обработки соответствующей информации или документов, содержащих вышеуказанную информацию в соответствии с законодательством РФ, после чего персональные данные уничтожаются.

7. Субъект персональных данных по письменному запросу имеет право на получение информации, касающейся обработки персональных данных (в соответствии с п.7 ст.14 ФЗ №152 «О персональных данных» от 27.07.2006).

8. Согласие может быть отозвано путем направления соответствующего письменного уведомления в адрес Оператора по почте заказным письмом, с уведомлением о вручении либо вручен лично под расписку представителю Оператора, после чего Оператор обязуется в течение 30 (тридцати) дней уничтожить персональные данные субъекта.

«____» _____20___г. _____ _____

подпись расшифровка подписи

Согласие на обработку персональных данных несовершеннолетнего (для участия в конкурсах и мероприятиях)

Я, _____,
фамилия, имя, отчество родителя (законного представителя) несовершеннолетнего субъекта персональных данных

паспорт _____ выдан _____ «__» _____г.,
серия, номер кем выдан дата выдачи

проживающий по адресу _____,
являясь родителем (законным представителем) субъекта персональных данных _____,
фамилия, имя, отчество несовершеннолетнего субъекта персональных данных

на основании _____,
(реквизиты документа, подтверждающего полномочия законного представителя)

проживающего по адресу_____,
свободно, своей волей и в своем интересе даю конкретное, информированное и сознательное согласие Муниципальному автономному учреждению дополнительного образования «Дворец пионеров и школьников им. Н.К. Крупской г. Челябинска», расположенному по адресу: 454080, Челябинская область, г.Челябинск, Свердловский пр., 59 (далее — Оператор), на обработку персональных данных субъектов (несовершеннолетнего ребенка и его родителя (законного представителя)) на следующих условиях:

1. Согласие дается мною в целях: участия в конкурсе (фестивале и др.) «_____»* (отправка заявки и иных документов для участия), публикации результатов участия в конкурсе (фестивале и др.) на официальных интернет-ресурсах организаторов конкурса (в том числе на официальном сайте МАУДО «ДПШ») с возможным использованием фото и видеоматериалов с изображением несовершеннолетнего субъекта персональных данных.

2. Настоящее согласие дается на осуществление следующих действий в отношении персональных данных субъектов, которые необходимы для достижения указанных выше целей, совершаемых с использованием средств автоматизации и без использования таких средств, включая без ограничения: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных, а также любых иных действий с учетом действующего законодательства РФ.

3. Перечень персональных данных несовершеннолетнего субъекта, передаваемых Оператору на обработку: фамилия, имя, отчество; пол; дата рождения; данные документа, удостоверяющего личность (вид, серия, номер, дата выдачи, наименование органа, выдавшего документ); данные о месте жительства; данные о местах обучения; состояние здоровья; фотография; сведения о посещаемости занятий; данные ИНН, данные страхового пенсионного свидетельства; контактный телефон; сведения о родителях (законных представителях) субъекта**.

4. Перечень персональных данных родителя (законного представителя) несовершеннолетнего субъекта, передаваемых Оператору на обработку: фамилия, имя, отчество; данные документа, удостоверяющего личность (вид, серия, номер, дата выдачи, наименование органа, выдавшего документ); данные о месте жительства; контактный телефон; место работы, должность, социальное положение семьи**.

5. Оператор имеет право передавать персональные данные несовершеннолетнего субъекта в Комитет по делам образования города Челябинска и иные организации*** для достижения указанных выше целей в случаях, установленных документами вышестоящих органов и законодательством РФ.

6. Настоящее согласие дается до достижения цели обработки персональных данных либо утраты правовых оснований обработки соответствующей информации или документов, содержащих вышеуказанную информацию в соответствии с законодательством РФ, после чего персональные данные уничтожаются.

7. Субъект персональных данных по письменному запросу имеет право на получение информации, касающейся обработки персональных данных (в соответствии с п.7 ст.14 ФЗ №152 «О персональных данных» от 27.07.2006).

8. Согласие может быть отозвано путем направления соответствующего письменного уведомления в адрес Оператора по почте заказным письмом, с уведомлением о вручении либо вручен лично под расписку представителю Оператора, после чего Оператор обязуется в течение 30 (тридцати) дней уничтожить персональные данные субъекта.

«____» _____20___г. _____ _____

подпись расшифровка подписи

*Указывается название конкурса, фестиваля и др.

**Для каждого мероприятия указывается необходимый перечень персональных данных субъекта.

***Указываются сторонние организации, если таковые имеются (МАУ ДОЛ «Солнечная поляна», ЧУ ДО ПАО «ММК» «Детский оздоровительно-образовательный комплекс» и др.)

Согласие на обработку персональных данных руководителя
(для участия в конкурсах и мероприятиях)

Я, _____,
фамилия, имя, отчество субъекта персональных данных

паспорт _____ выдан _____ «__» _____г.,
серия, номер кем выдан дата выдачи

проживающий по адресу _____,
свободно, своей волей и в своем интересе даю конкретное, информированное и сознательное согласие Муниципальному автономному учреждению дополнительного образования «Дворец пионеров и школьников им. Н.К. Крупской г. Челябинска», расположенному по адресу: 454080, Челябинская область, г.Челябинск, Свердловский пр., 59 (далее — Оператор), на обработку моих персональных данных на следующих условиях:

1. Согласие дается мною в целях: исполнения обязанностей ответственного за сопровождение детей в «_____»*, публикации результатов участия в конкурсе (фестивале и др.) на официальных интернет-ресурсах организаторов конкурса (в том числе на официальном сайте МАУДО «ДПШ») с возможным использованием фото и видеоматериалов с моим изображением.

2. Настоящее согласие дается на осуществление следующих действий в отношении персональных данных субъекта, которые необходимы для достижения указанных выше целей, совершаемых с использованием средств автоматизации и без использования таких средств, включая без ограничения: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных, а также любых иных действий с учетом действующего законодательства РФ.

3. Перечень персональных данных субъекта, передаваемых Оператору на обработку: фамилия, имя, отчество; данные документа, удостоверяющего личность (вид, серия, номер, дата выдачи, наименование органа, выдавшего документ); данные о месте жительства; контактный телефон; место работы, должность**.

4. Оператор имеет право передавать персональные данные несовершеннолетнего субъекта в Комитет по делам образования города Челябинска и иные организации*** для достижения указанных выше целей в случаях, установленных документами вышестоящих органов и законодательством РФ.

5. Настоящее согласие дается до достижения цели обработки персональных данных либо утраты правовых оснований обработки соответствующей информации или документов, содержащих вышеуказанную информацию в соответствии с законодательством РФ, после чего персональные данные уничтожаются.

6. Субъект персональных данных по письменному запросу имеет право на получение информации, касающейся обработки персональных данных (в соответствии с п.7 ст.14 ФЗ №152 «О персональных данных» от 27.07.2006).

7. Согласие может быть отозвано путем направления соответствующего письменного уведомления в адрес Оператора по почте заказным письмом, с уведомлением о вручении либо вручен лично под расписку представителю Оператора, после чего Оператор обязуется в течение 30 (тридцати) дней уничтожить персональные данные субъекта.

«____» _____20___г. _____ _____

подпись расшифровка подписи

*Указывается название конкурса, фестиваля и др.

**Для каждого мероприятия указывается необходимый перечень персональных данных субъекта.

***Указываются сторонние организации, если таковые имеются (МАУ ДОЛ «Солнечная поляна», ЧУ ДО ПАО «ММК» «Детский оздоровительно-образовательный комплекс» и др.)

Согласие на обработку персональных данных члена оргкомитета (рабочей группы, жюри, экспертной группы) конкурса

Я, _____,
фамилия, имя, отчество субъекта персональных данных

паспорт _____ выдан _____ «__» _____г.,
серия, номер кем выдан дата выдачи

проживающий по адресу _____,
свободно, своей волей и в своем интересе даю конкретное, информированное и сознательное согласие Муниципальному автономному учреждению дополнительного образования «Дворец пионеров и школьников им. Н.К. Крупской г. Челябинска», расположенному по адресу: 454080, Челябинская область, г.Челябинск, Свердловский пр., 59 (далее — Оператор), на обработку моих персональных данных на следующих условиях:

1. Согласие дается мною в целях: исполнения обязанностей члена оргкомитета (рабочей группы, жюри, экспертной группы) конкурса (фестиваля и др.) «_____»*, публикации результатов конкурса (фестиваля и др.) на официальных интернет-ресурсах организаторов конкурса (в том числе на официальном сайте МАУДО «ДПШ») с возможным использованием фото и видеоматериалов с моим изображением.

2. Настоящее согласие дается на осуществление следующих действий в отношении персональных данных субъекта, которые необходимы для достижения указанных выше целей, совершаемых с использованием средств автоматизации и без использования таких средств, включая без ограничения: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных, а также любых иных действий с учетом действующего законодательства РФ.

3. Перечень персональных данных субъекта, передаваемых Оператору на обработку: фамилия, имя, отчество; данные документа, удостоверяющего личность (вид, серия, номер, дата выдачи, наименование органа, выдавшего документ); данные о месте жительства; контактный телефон; место работы, должность, адрес электронной почты**.

4. Оператор имеет право передавать персональные данные субъекта в Комитет по делам образования города Челябинска и иные организации*** для достижения указанных выше целей в случаях, установленных документами вышестоящих органов и законодательством РФ.

5. Настоящее согласие дается до достижения цели обработки персональных данных либо утраты правовых оснований обработки соответствующей информации или документов, содержащих вышеуказанную информацию в соответствии с законодательством РФ, после чего персональные данные уничтожаются.

6. Субъект персональных данных по письменному запросу имеет право на получение информации, касающейся обработки персональных данных (в соответствии с п.7 ст.14 ФЗ №152 «О персональных данных» от 27.07.2006).

7. Согласие может быть отозвано путем направления соответствующего письменного уведомления в адрес Оператора по почте заказным письмом, с уведомлением о вручении либо вручен лично под расписку представителю Оператора, после чего Оператор обязуется в течение 30 (тридцати) дней уничтожить персональные данные субъекта.

«____» _____20___г. _____ _____

подпись расшифровка подписи

*Указывается название конкурса, фестиваля и др.

**Для каждого мероприятия указывается необходимый перечень персональных данных субъекта.

***Указываются сторонние организации, если таковые имеются (МАУ ДОЛ «Солнечная поляна», ЧУ ДО ПАО «ММК» «Детский оздоровительно-образовательный комплекс» и др.)

Согласие на обработку персональных данных соискателя

Я, _____,
фамилия, имя, отчество субъекта персональных данных

паспорт _____ выдан _____ «__» _____г.,
серия, номер кем выдан дата выдачи

проживающий по адресу _____,
свободно, своей волей и в своем интересе даю конкретное, информированное и сознательное согласие Муниципальному автономному учреждению дополнительного образования «Дворец пионеров и школьников им. Н.К. Крупской г. Челябинска», расположенному по адресу: 454080, Челябинская область, г.Челябинск, Свердловский пр., 59 (далее — Оператор), на обработку моих персональных данных на следующих условиях:

1. Согласие дается в целях принятия решения о трудоустройстве.

2. Настоящее согласие дается на осуществление следующих действий в отношении персональных данных субъекта, которые необходимы для достижения указанных выше целей, совершаемых с использованием средств автоматизации и без использования таких средств, включая без ограничения: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных, а также любых иных действий с учетом действующего законодательства РФ.

3. Перечень персональных данных субъекта, передаваемых Оператору на обработку: фамилия, имя, отчество; образование; специальность; профессия; предыдущий опыт работы; стаж по специальности; контактный телефон; адрес электронной почты.

4. Оператор имеет право передавать персональные данные субъекта в иные учреждения в соответствии с законодательством Российской Федерации.

5. Настоящее согласие дается до достижения цели обработки персональных данных либо утраты правовых оснований обработки соответствующей информации или документов, содержащих вышеуказанную информацию в соответствии с законодательством РФ, после чего персональные данные уничтожаются.

6. Субъект персональных данных по письменному запросу имеет право на получение информации, касающейся обработки персональных данных (в соответствии с п.7 ст.14 ФЗ №152 «О персональных данных» от 27.07.2006).

7. Согласие может быть отозвано путем направления соответствующего письменного уведомления в адрес Оператора по почте заказным письмом, с уведомлением о вручении либо вручен лично под расписку представителю Оператора, после чего Оператор обязуется в течение 30 (тридцати) дней уничтожить персональные данные субъекта.

«____» _____20___г. _____ _____
подпись расшифровка подписи

Согласие на обработку персональных данных работника

Я, _____,
фамилия, имя, отчество субъекта персональных данных

паспорт _____ выдан _____ «__» _____г.,
серия, номер кем выдан дата выдачи

проживающий по адресу _____,
свободно, своей волей и в своем интересе даю конкретное, информированное и сознательное согласие Муниципальному автономному учреждению дополнительного образования «Дворец пионеров и школьников им. Н.К. Крупской г. Челябинска», расположенному по адресу: 454080, Челябинская область, г.Челябинск, Свердловский пр., 59 (далее — Оператор), на обработку моих персональных данных на следующих условиях:

1. Согласие дается мною в целях: осуществления трудовых (договорных) отношений с МАУДО «ДПШ», передачи данных в организации, указанные в п.4, размещения информации на официальном сайте МАУДО «ДПШ».

2. Настоящее согласие дается на осуществление следующих действий в отношении моих персональных данных, которые необходимы для достижения указанных выше целей, совершаемых с использованием средств автоматизации и без использования таких средств, включая, без ограничения: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение, а также любых иных действий с учетом действующего законодательства РФ.

3. Типовой перечень персональных данных, передаваемых Оператору на обработку:

1) фамилия, имя, отчество;
2) ИНН;
3) СНИЛС (№ страхового пенсионного свидетельства);
4) табельный номер;
5) пол;
6) номер, дата трудового договора;
7) дата рождения;
8) место рождения;
9) гражданство;
10) наименование и степень знания иностранного языка;
11) образование (среднее (полное) общее, начальное профессиональное, среднее профессиональное, высшее профессиональное, аспирантура, адъюнктура, докторантура);
12) наименование образовательного учреждения;
13) наименование, серия, номер, дата выдачи, направление или специальность, код по ОКСО, ОКИН документа об образовании, о квалификации или наличии специальных знаний;
14) профессия (в т.ч. по ОКПДТР);
15) стаж работы;
16) состояние в браке;
17) состав семьи, с указанием степени родства, фамилии, имени, отчества, года рождения ближайших родственников;

18) данные документа, удостоверяющего личность (вид, серия, номер, дата выдачи, наименование органа, выдавшего документ);

19) адрес и дата регистрации;

20) фактический адрес места жительства;

21) телефон;

22) сведения о воинском учете (категория запаса, воинское звание, состав (профиль), полное кодовое обозначение ВУС, категория годности к военной службе, наименование военного комиссариата по месту жительства, состоит на воинском учете, отметка о снятии с учета);

23) дата приема на работу;

24) характер работы;

25) вид работы (основной, по совместительству);

26) структурное подразделение;

27) занимаемая должность (специальность, профессия), разряд, класс (категория) квалификации;

28) ранее занимаемая должность;

29) тарифная ставка (оклад), надбавка, руб.;

30) основание трудоустройства;

31) личная подпись сотрудника;

32) фотография;

33) сведения об аттестации (дата, решение, номер и дата документа, основание);

34) сведения о профессиональной подготовке (дата начала и окончания переподготовки, специальность (направление, профессия), наименование, номер, дата документа, свидетельствующего о переподготовке, основание переподготовки);

35) сведения о наградах, поощрениях, почетных званиях (наименование, номер, дата награды);

36) сведения об отпусках (вид, период работы, количество дней, дата начала и окончания, основание);

37) сведения о социальных льготах, на которые работник имеет право в соответствии с законодательством РФ (наименование льготы, номер, дата выдачи документа, основание);

38) сведения об увольнении (основание, дата, номер и дата приказа);

39) объем работы;

40) сведения о доходах;

41) сведения из трудовой книжки;

42) сведения из личной медицинской книжки;

43) сведения из водительского удостоверения.

4. Организации, которым Оператор предоставляет персональные данные субъекта – банки, налоговые органы, отделения пенсионного фонда, фонда социального страхования, фонда обязательного медицинского страхования, органы внутренних дел, учреждения образования, здравоохранения, культуры.

5. Настоящее согласие дается до достижения цели обработки персональных данных либо утраты правовых оснований обработки соответствующей информации или документов, содержащих вышеуказанную информацию в соответствии с законодательством РФ.

6. Субъект персональных данных по письменному запросу имеет право на получение информации, касающейся обработки персональных данных (в соответствии с п.7 ст.14 ФЗ №152 «О персональных данных» от 27.07.2006).

7. Согласие может быть отозвано путем направления соответствующего письменного уведомления в адрес Оператора по почте заказным письмом, с уведомлением о вручении либо вручен лично под расписку представителю Оператора, после чего Оператор обязуется в течение 30 (тридцати) дней уничтожить персональные данные субъекта.

8. Обязуюсь сообщать в трехдневный срок об изменении места жительства, контактных телефонов, паспортных, документных и иных данных. Об ответственности за достоверность представленных персональных данных предупрежден(а).

«____» _____20___г. _____ _____

подпись расшифровка подписи

Приложение 24
к приказу МАУДО «ДПШ»
от 19.01.26 № 22-од

Перечень
мест хранения материальных носителей защищаемой информации

№ п/п	Носитель информации	Должность допущенного должностного лица	Место расположения
1.	Личные дела работников	Директор, специалист по кадрам, главный бухгалтер, заместитель главного бухгалтера, ведущий бухгалтер, бухгалтер, заведующий канцелярией, ответственный за организацию обработки персональных данных, ответственный за обеспечение безопасности персональных данных	Сейф отдела кадров (Каб. №10), сейф канцелярии (Каб. №11)
2.	Документы по воинскому учету	Директор, специалист по кадрам, заведующий канцелярией, ответственный за организацию обработки персональных данных	Сейф отдела кадров (Каб. №10), сейф канцелярии (Каб. №11)
3.	Книга учета движения трудовых книжек и вкладышей в них	Директор, специалист по кадрам, ответственный за организацию обработки персональных данных	Шкаф отдела кадров (Каб. №10)
4.	Журнал регистрации трудовых договоров и изменений к ним	Директор, специалист по кадрам, ответственный за организацию обработки персональных данных	Шкаф отдела кадров (Каб. №10)
5.	Книга регистрации приказов	Директор, специалист по кадрам, заведующий канцелярией, ответственный за организацию обработки персональных данных	Шкаф отдела кадров (Каб. №10)
6.	Документы первичного бухгалтерского учета	Директор, главный бухгалтер, бухгалтер, ответственный за организацию обработки персональных данных	Шкаф бухгалтерии (Каб. №23)
7.	Договоры с контрагентами	Директор, главный бухгалтер, бухгалтер, контрактный управляющий, ответственный за организацию обработки персональных данных	Шкаф кабинета контрактного управляющего (Каб. №12)
8.	Личные дела обучающихся	Директор, секретарь, руководитель учебного отдела, методист, ответственный за организацию обработки персональных данных, документовед, ответственный за обеспечение безопасности персональных данных	Сейф кабинета приемной комиссии (Каб. №24), сейф методического кабинета спортивного комплекса (Каб. №207)

9.	Журнал заявлений на обучение от обучающихся и (или) родителей (законных представителей) несовершеннолетних обучающихся	Директор, работники структурного подразделения, ответственный за организацию обработки персональных данных	Шкаф кабинета руководителя структурного подразделения
10.	Журнал инструктажа обучающихся по технике безопасности	Директор, работники структурного подразделения, ответственный за организацию обработки персональных данных	Шкаф кабинета руководителя структурного подразделения
11.	Журнал инструктажа по антитеррористической защищенности	Директор, работники структурного подразделения, ответственный за организацию обработки персональных данных	Шкаф кабинета руководителя структурного подразделения
12.	Журнал регистрации противопожарного инструктажа	Директор, работники структурного подразделения, ответственный за организацию обработки персональных данных	Шкаф кабинета руководителя структурного подразделения
13.	Журнал регистрации инструктажей на рабочем месте	Директор, работники структурного подразделения, ответственный за организацию обработки персональных данных	Шкаф кабинета руководителя структурного подразделения
14.	Годовые отчеты по успеваемости обучающихся	Директор, руководитель учебного отдела, ответственный за организацию обработки персональных данных	Шкаф кабинета руководителя учебного отдела
15.	Журнал учета выдачи медицинских книжек и направлений на медицинский осмотр	Директор, медицинский работник, ответственный за организацию обработки персональных данных	Шкаф медицинского кабинета (Каб. №202)

Приложение 25
к приказу МАУДО «ДПШ»
от 19.01.26 № 22-д

Перечень
информационных систем (ИС)

№ п/п	Тип ИС	Наименование ИС	Уровень / класс защищенности	Местоположение
1.	ИСПДн	«Бухгалтерия и кадры»	УЗ 4	454080, Россия, Челябинская область, г. Челябинск, Свердловский пр.59
2.	ИСПДн	«Воспитанники»	УЗ 4	454080, Россия, Челябинская область, г. Челябинск, Свердловский пр.59

Приложение 26
к приказу МАУДО «ДПШ»
от 19.01.26 № 22-ОД

Перечень
должностей, доступ которых к защищаемой информации необходим для выполнения служебных (трудовых) обязанностей

№ п/п	Должность допущенного должностного лица	Метод обработки	Наименование информационной системы
1.	Директор	автоматизированная и неавтоматизированная обработка	«Воспитанники», «Бухгалтерия и кадры»
2.	Первый заместитель директора, ответственный за организацию обработки персональных данных	автоматизированная и неавтоматизированная обработка	«Воспитанники», «Бухгалтерия и кадры»
3.	Заместитель директора по обеспечению комплексной безопасности	автоматизированная и неавтоматизированная обработка	«Воспитанники», «Бухгалтерия и кадры»
4.	Заместитель директора по инновационному развитию	автоматизированная и неавтоматизированная обработка	«Бухгалтерия и кадры»
5.	Заместитель директора по культурно-воспитательной деятельности	автоматизированная и неавтоматизированная обработка	«Воспитанники», «Бухгалтерия и кадры»
6.	Заместитель директора по обеспечению качества образования	автоматизированная и неавтоматизированная обработка	«Воспитанники», «Бухгалтерия и кадры»
7.	Заместитель директора по административно-хозяйственной части	автоматизированная и неавтоматизированная обработка	«Бухгалтерия и кадры»
8.	Главный бухгалтер	автоматизированная и неавтоматизированная обработка	«Воспитанники», «Бухгалтерия и кадры»
9.	Агент по снабжению	неавтоматизированная обработка	«Бухгалтерия и кадры»
10.	Архивариус	автоматизированная и неавтоматизированная обработка	«Воспитанники», «Бухгалтерия и кадры»
11.	Бухгалтер	автоматизированная и неавтоматизированная обработка	«Воспитанники», «Бухгалтерия и кадры»
12.	Ведущий бухгалтер	автоматизированная и	«Воспитанники»,

№ п/п	Должность допущенного должностного лица	Метод обработки	Наименование информационной системы
		неавтоматизированная обработка	«Бухгалтерия и кадры»
13.	Делопроизводитель	автоматизированная и неавтоматизированная обработка	«Воспитанники», «Бухгалтерия и кадры»
14.	Документовед	неавтоматизированная обработка	«Воспитанники»
15.	Заведующий канцелярией	автоматизированная и неавтоматизированная обработка	«Бухгалтерия и кадры»
16.	Заведующий хозяйством	автоматизированная и неавтоматизированная обработка	«Бухгалтерия и кадры»
17.	Заместитель главного бухгалтера	автоматизированная и неавтоматизированная обработка	«Воспитанники», «Бухгалтерия и кадры»
18.	Звукорежиссер	неавтоматизированная обработка	«Воспитанники»
19.	Контрактный управляющий	автоматизированная и неавтоматизированная обработка	«Бухгалтерия и кадры»
20.	Концертмейстер	неавтоматизированная обработка	«Воспитанники»
21.	Методист	автоматизированная и неавтоматизированная обработка	«Воспитанники»
22.	Педагог дополнительного образования	автоматизированная и неавтоматизированная обработка	«Воспитанники»
23.	Педагог-организатор	автоматизированная и неавтоматизированная обработка	«Воспитанники»
24.	Педагог-психолог	автоматизированная и неавтоматизированная обработка	«Воспитанники»
25.	Программист	автоматизированная и неавтоматизированная обработка	«Воспитанники», «Бухгалтерия и кадры»
26.	Режиссер	неавтоматизированная обработка	«Воспитанники»
27.	Социальный педагог	автоматизированная и неавтоматизированная обработка	«Воспитанники»

№ п/п	Должность допущенного должностного лица	Метод обработки	Наименование информационной системы
28.	Специалист по ГО и ЧС	неавтоматизированная обработка	«Воспитанники»
29.	Специалист по кадрам	автоматизированная и неавтоматизированная обработка	«Бухгалтерия и кадры»
30.	Специалист по охране труда	автоматизированная и неавтоматизированная обработка	«Бухгалтерия и кадры»
31.	Старший методист	автоматизированная и неавтоматизированная обработка	«Воспитанники», «Бухгалтерия и кадры»
32.	Тренер-преподаватель	автоматизированная и неавтоматизированная обработка	«Воспитанники»

Приложение 27
к приказу МАУДО «ДПШ»
от 19.01.2026 № 22-Д

Состав
комиссии по вопросам обработки персональных данных

№ п/п	ФИО допущенного должностного лица	Должность допущенного должностного лица
1.	Смирнова Юлия Викторовна	Директор
2.	Завьялов Антон Александрович	Первый заместитель директора
3.	Павлухин Дмитрий Владимирович	Заместитель директора по обеспечению комплексной безопасности
4.	Дегтярева Наталья Александровна	Главный бухгалтер
5.	Артишевская Инна Дмитриевна	Заместитель директора по обеспечению качества образования
6.	Незговорова Елена Викторовна	Ведущий бухгалтер
7.	Осипова Анна Саввична	Руководитель учебного отдела

Приложение 28
к приказу МАУДО «ДШИ»
от 19.01.26 № 22-д

План
внутренних проверок
состояния защиты информационных систем персональных данных

№ п/п	Мероприятие	Периодичность	Исполнитель	Отметка об исполнении
1.	Контроль за принимаемыми мерами по обеспечению безопасности персональных данных	Постоянно	Ответственный за организацию обработки персональных данных	
2.	Внесение изменений в ранее поданное Уведомление об обработке персональных данных	В течение 10 дней в случае изменения сведений	Ответственный за организацию обработки персональных данных	
3.	Контроль за соблюдением режима безопасности помещений, в которых размещена информационная система	Постоянно	Ответственный за организацию обработки персональных данных	Журнал учета ключей от сейфов и помещений, Журнал проверок исправности сигнализации, Журнал учета работ в ИС
4.	Контроль за выполнением мероприятий антивирусной защиты	Еженедельно	Ответственный за обеспечение безопасности ПДн в ИСПДн	
5.	Контроль сохранности носителей защищаемой информации	Ежеквартально	Ответственный за организацию обработки персональных данных	Журнал учета съемных носителей информации
6.	Проверка актуальности прав разграничения доступа пользователей ИСПДн.	Ежемесячно	Ответственный за обеспечение безопасности ПДн в ИСПДн	
7.	Проверка актуальности перечня обрабатываемых персональных данных	Ежемесячно	Ответственный за организацию обработки персональных данных	Перечень обрабатываемых персональных данных
8.	Повышение осведомленности сотрудников, участвующих в обработке персональных данных с изменением	Ежегодно	Ответственный за организацию обработки персональных данных	

№ п/п	Мероприятие	Периодичность	Исполнитель	Отметка об исполнении
	законодательства и внутренних локальных актов по персональным данным			
9.	Проверка актуальности сертификатов соответствия на используемые средства защиты информации	Ежегодно	Ответственный за обеспечение безопасности ПДн в ИСПДн	Журнал учёта средств защиты информации, эксплуатационной и технической документации к ним
10.	Контроль над соблюдением режима защиты при подключении к сетям общего пользования и (или) международного обмена	Еженедельно	Ответственный за обеспечение безопасности ПДн в ИСПДн	Журнал учета работ в ИС
11.	Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты информации	Ежегодно	Ответственный за организацию обработки персональных данных	Журнал учета работ в ИС
12.	Контроль за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах ИС	Ежемесячно	Ответственный за обеспечение безопасности ПДн в ИСПДн	Журнал учета работ в ИС
13.	Контроль установленного (инсталлированного) в информационной системе программного обеспечения на предмет соответствия его перечню программного обеспечения	Ежемесячно	Ответственный за обеспечение безопасности ПДн в ИСПДн	Журнал учета работ в ИС
14.	Контроль наличия и местонахождения машинных носителей информации.	Ежемесячно	Ответственный за обеспечение безопасности ПДн в ИСПДн	Журнал учета работ в ИС
15.	Контроль наличия и местонахождения бумажных носителей информации.	Ежемесячно	Ответственный за организацию обработки персональных данных	
16.	Контроль компонентов информационной системы (автоматизированных рабочих мест, серверов, других средств вычислительной техники) на наличие вредоносных компьютерных программ	Постоянно	Ответственный за обеспечение безопасности ПДн в ИСПДн	Журнал учета работ в ИС

№ п/п	Мероприятие	Периодичность	Исполнитель	Отметка об исполнении
	(вирусов)			
17.	Контроль за обеспечением резервного копирования	Ежемесячно	Ответственный за обеспечение безопасности ПДн в ИСПДн	Журнал учета работ в ИС
18.	Контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации	Ежемесячно	Ответственный за обеспечение безопасности ПДн в ИСПДн	Журнал учета работ в ИС
19.	Организация анализа и пересмотра имеющихся угроз безопасности ЗИ, а также предсказание появления новых угроз	Ежегодно	Ответственный за обеспечение безопасности ПДн в ИСПДн	Журнал учета работ в ИС
20.	Поддержание в актуальном состоянии организационно-распорядительных документов	Ежемесячно	Ответственный за организацию обработки персональных данных	Журнал учета работ в ИС
21.	Проведение оценки эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных	Раз в 3 года	Ответственный за организацию обработки персональных данных	Акт оценки эффективности мер по обеспечению безопасности персональных данных