

Районный отдел образования
администрации Павинского муниципального района

ПРИКАЗ

от 26.01.2022 года № 9

Об утверждении документов,
регламентирующих работу с персональными данными
в районном отделе образования
администрации Павинского муниципального района

В соответствии с требованиями Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», постановления правительства Российской Федерации от 21.03.2021 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», в целях обеспечения безопасности обработки персональных данных, обрабатываемых в районном отделе образования администрации Павинского муниципального района,

ПРИКАЗЫВАЮ:

1. Назначить ответственными лицами за обработку персональных данных в районном отделе образования администрации Павинского муниципального района:
 - 1.1 Лыхину Татьяну Леонидовну, заместителя заведующего РОО;
 - 1.2 Хомякову Елену Витальевну, ведущего специалиста-эксперта РОО;
 - 1.3 Киселеву Алесю Викторовну, ведущего специалиста-эксперта РОО;
 - 1.4 Павлову Анну Алексеевну, ведущего специалиста-эксперта РОО;
2. Утвердить должностную инструкцию ответственных лиц за обработку персональных данных в районном отделе образования администрации Павинского муниципального района (приложение №1).
3. Утвердить документы, регламентирующие работу с персональными данными в районном отделе образования администрации Павинского муниципального района:
 - 3.1 Положение об обработке персональных данных в районном отделе образования администрации Павинского муниципального района (приложение № 2);

- 3.2 Правила рассмотрения запросов субъектов персональных данных или их представителей в районном отделе образования администрации Павинского муниципального района (приложение № 3);
- 3.3 Правила работы с обезличенными персональными данными, обрабатываемыми в районном отделе образования администрации Павинского муниципального района (приложение № 4);
- 3.4 Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям нормативных документов (приложение № 5);
- 3.5 Правила работы с информационными системами районного отдела образования администрации Павинского муниципального района (приложение № 6);
- 3.6 Порядок доступа в помещения районного отдела образования администрации Павинского муниципального района, в которых ведется обработка персональных данных (приложение № 7);
- 3.7 Уведомление об уничтожении, изменении, прекращении обработки, устранении нарушений, допущенных при обработке персональных данных (приложение № 8);

4. Контроль за исполнением настоящего приказа оставляю за собой.

Заведующий районным отделом образования

Т.В. Лаптева

С приказом ознакомлены:



Т.Л. Лыхина

Е.В. Хомякова

А.В. Киселева

А.А. Павлова

**Должностная инструкция
ответственных за организацию обработки персональных данных
в районном отделе образования
администрации Павинского муниципального района**

1. Общие положения

1.1. Должностные лица районного отдела образования администрации Павинского муниципального района (далее РОО), ответственные за организацию обработки персональных данных, назначаются и освобождаются заведующим РОО.

1.2. Должностные лица, ответственные за организацию обработки персональных данных, должны руководствоваться в своей деятельности Федеральным законом от 27 июля 2006 года N 152-ФЗ "О персональных данных", Постановлением Правительства Российской Федерации от 15 сентября 2008 года N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации" и другими нормативными правовыми актами, а так же настоящей должностной инструкцией.

1.3. Инструкция определяет ответственность, обязанности и права лиц, назначенных ответственными за организацию обработки персональных данных.

2. Должностные обязанности

Должностные лица, ответственные за организацию обработки персональных данных, выполняют следующие обязанности:

- а) предоставляют субъекту персональных данных по его просьбе информацию;
- б) осуществляют внутренний контроль за соблюдением требований законодательства РФ при обработке персональных данных в РОО, в том числе требований к защите персональных данных;
- в) организуют прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществляют контроль за приемом и обработкой таких обращений и запросов;
- д) разъясняют субъекту персональных данных юридические последствия отказа предоставления его персональных данных.

3. Права

Должностные лица, ответственные за организацию обработки персональных данных, вправе:

- а) принимать решения в пределах своей компетенции;
- б) запрашивать и получать в установленном порядке от субъектов персональных данных или их представителей сведения, содержащие персональные данные;
- в) распоряжаться полученными персональными данными в пределах, установленных законодательством;
- г) в установленном порядке пользоваться системами связи, информационными

базами данных и иными носителя информации РОО.

4. Ответственность

4.1. Должностные лица, ответственные за организацию обработки персональных данных, в соответствии со своими полномочиями владеющие информацией о субъектах персональных данных, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки, использования, хранения и передачи персональных данных.

4.2. Должностные лица, виновные в нарушении установленного законом порядка сбора, хранения, использования, распространения или защиты персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством.

С должностной инструкцией ознакомлены:

_____	_____
(подпись)	(фамилия имя, отчество)

"__" _____ 20__ года

_____	_____
(подпись)	(фамилия имя, отчество)

"__" _____ 20__ года

_____	_____
(подпись)	(фамилия имя, отчество)

"__" _____ 20__ года

_____	_____
(подпись)	(фамилия имя, отчество)

"__" _____ 20__ года

**Положение
об обработке персональных данных в районном отделе образования
администрации Павинского муниципального района**

1. Общие положения

1.1. Настоящее Положение принято в целях обеспечения защиты персональных данных работников районного отдела образования администрации Павинского муниципального района (оператора ПДн), а также физических лиц, состоящих в договорных отношениях с РОО.

1.2. Положение определяет политику оператора в отношении обработки персональных данных, права и обязанности оператора и субъектов персональных данных, порядок использования персональных данных в целях реализации требований действующего законодательства и исполнения служебных обязанностей, а также порядок взаимодействия по вопросам сбора, документирования, хранения и уничтожения персональных данных.

1.3. Настоящее Положение разработано на основании и во исполнение части 1 статьи 23, статьи 24 Конституции Российской Федерации, Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Федерального закона от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», положений главы 14 Трудового кодекса Российской Федерации «Защита персональных данных работников», постановления Правительства РФ от 21 марта 2012 №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных», постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и иных нормативно-правовых актов.

1.4. Персональные данные обрабатываются с согласия субъекта персональных данных, если иное не определено федеральным законом. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме.

1.5. Специальные категории персональных данных, касающиеся расовой и национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья обрабатываются в случаях, предусмотренных ст. 10 Федерального закона от 26.07.2006 г. № 152-ФЗ «О персональных данных», только при наличии письменного согласия субъекта персональных данных.

1.6. Обработка персональных данных в целях оказания услуг с помощью средств связи допускается только при условии предварительного согласия субъекта персональных данных. Указанная обработка персональных данных признается осуществляемой без предварительного согласия субъекта персональных данных, если оператор не докажет, что такое согласие было получено.

1.7. Обработка персональных данных в РОО ограничивается достижением конкретных, заранее определенных и законных целей. Содержание и объём обрабатываемых персональных данных соответствуют заявленным целям обработки. Обрабатываемые персональные данные не являются избыточными по отношению к

заявленным целям их обработки. Обработка персональных данных, несовместимая с целями сбора персональных данных, не допускается.

2. Основные термины и определения

Для целей настоящего Положения используются следующие основные понятия:

персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

оператор - орган исполнительной власти, 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;

автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

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;

обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

3. Меры по защите персональных данных

В РОО разработаны и внедрены следующие меры для обеспечения выполнения предусмотренных действующим законодательством обязанностей по предотвращению несанкционированного доступа или неправомерного использования, утраты информации, содержащей персональные данные работников:

- назначены ответственные за организацию обработки персональных данных;
- определены Перечни категорий персональных данных, обрабатываемых в РОО (Приложение 1);
- определен Перечень должностей, имеющих доступ к персональным данным (Приложение 2);
- назначены ответственные за обеспечение безопасности персональных данных при работе в информационных системах;
- определены места хранения материальных носителей персональных данных в РОО;
- разработан и утвержден порядок доступа работников РОО в помещения, где обрабатываются персональные данные;

- реализованы требования по парольной и иной защите доступа к информационным ресурсам (длина не менее шести знаков, регулярная смена паролей);
- определен порядок размещения мониторов на рабочих местах пользователей, исключающий просмотр визуальной информации посторонними лицами;
- обеспечивается защита от воздействия вредоносных программ и программно-математических воздействий (антивирусная защита, администрирование);
- реализована передача обрабатываемых персональных данных по общедоступной телекоммуникационной сети (Интернет) с использованием сертифицированных программных средств защиты информации;
- организован контроль выполнения условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный доступ к ним.

4. Обработка персональных данных сотрудников РОО, а так же руководителей образовательных учреждений

4.1. Обработка персональных данных сотрудников осуществляется в соответствии с требованиями трудового, налогового, пенсионного и иного законодательства.

4.2. В соответствии с требованиями Федерального закона Российской Федерации от 24.07.2004 № 79-ФЗ «О государственной гражданской службе в РФ» и ст. 65 Трудового кодекса Российской Федерации при заключении трудового договора лицо, поступающее на работу, предъявляет работодателю:

- паспорт или иной документ, удостоверяющий личность;
- трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства;
- страховое свидетельство государственного пенсионного страхования;
- документы воинского учета - для военнообязанных и лиц, подлежащих призыву на военную службу;
- документы об образовании, о квалификации или наличии специальных знаний - при поступлении на работу, требующую специальных знаний или специальной подготовки;
- справку о наличии (отсутствии) судимости - при поступлении на работу, связанную с деятельностью, к осуществлению которой не допускаются лица, имеющие или имевшие судимость, подвергающиеся или подвергавшиеся уголовному преследованию.

В отдельных случаях может предусматриваться необходимость предъявления дополнительных документов.

Запрещается требовать от лица, поступающего на работу, документы помимо предусмотренных Трудовым кодексом и иными федеральными законами, регламентирующими деятельность государственного гражданского служащего, указами Президента Российской Федерации и постановлениями Правительства Российской Федерации.

4.3. Персональные данные работника предоставляются самим работником. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

4.4. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие.

4.5. Работник обязан предоставлять работодателю достоверную персональную информацию. При изменении персональных данных работник должен письменно уведомить об этом работодателя в срок, не превышающий 14 дней. Работодатель имеет право запрашивать у работника дополнительные сведения и документы, подтверждающие их достоверность.

4.6. Работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия (Приложение 3, Приложение 4).

4.7. Работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных Федеральным законом РФ от 27.07.2006 № 152-ФЗ «О персональных данных» или иными федеральными законами.

4.8. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных (Приложение 5). В случае отзыва субъектом персональных данных согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в федеральном законодательстве.

4.9. Для изучения и оценки возможности приема на работу в РОО, кандидаты на вакантные должности проходят собеседование и иные, предусмотренные законодательством процедуры. В случае принятия положительного решения, кандидат заполняет анкету установленной формы и оформляется на работу.

Персональные данные кандидатов обрабатываются без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации.

Порядок обработки персональных данных без использования средств автоматизации определен Правилами обработки персональных данных, осуществляемой без использования средств автоматизации.

4.10. При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения.

5. Обработка персональных данных физических лиц и контрагентов

5.1. Оператор ПДн в случаях предусмотренных законодательством имеет право обрабатывать персональные данные физических лиц и контрагентов.

5.2. При заключении договора с физическим лицом (субъект ПДн) или контрагентом (должностное лицо) согласие на обработку своих персональных данных, предоставленных в разделах договора не требуется.

5.3. Персональные данные, полученные оператором в связи с заключением договора, стороной которого является субъект персональных данных (физическое либо должностное лицо), не распространяются и не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного.

6. Порядок хранения и использования персональных данных

6.1. Хранение персональных данных работников осуществляется на бумажных носителях, а при необходимости ведения централизованных учетов, устанавливаемых федеральным законодательством, и на электронных носителях.

6.2. Доступ к персональным данным, хранящимся на электронных носителях, а также к программному обеспечению регламентирован и осуществляется при введении пароля, использования электронной подписи иных средств защиты от несанкционированного доступа.

6.3. Документы (на бумажных носителях), содержащие ПДн, хранятся в шкафах работников, ответственных за ведение и хранение таких документов.

6.4. Помещения, в которых хранятся персональные данные работников, оборудуются средствами физической защиты (двери, замки).

6.5. Обработка персональных данных в РОО осуществляется исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества, исполнения работодателем договорных обязательств. |

6.6. Допуск к персональным данным разрешен должностным лицам, включенным в Перечень должностей, которым персональные данные необходимы для выполнения конкретных трудовых функций.

6.7. К персональным данным, обрабатываемым в РОО, могут допускаться работники контрольно-ревизионных органов при наличии документов, являющихся основанием к работе с персональными данными.

6.8. Работники, обрабатывающие персональные данные с использованием и без использования средств автоматизации, обязаны обеспечивать их безопасность от несанкционированного доступа к ним и копирования.

6.9. Работники, допущенные к обработке персональных данных, обязаны:

- осуществлять передачу персональных данных работников в пределах организации в соответствии с Перечнем должностей;

- предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено;

- разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;

- передавать персональные данные работника представителям работников в порядке, установленном законодательством Российской Федерации, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

6.10. Работникам, допущенным к обработке персональных данных, запрещается:

- сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных законодательством Российской Федерации;

- сообщать персональные данные работника в коммерческих целях без его письменного согласия;

- запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции.

6.11. Защита персональных данных работников от их неправомерного использования или утраты обеспечивается работодателем за счет его средств в порядке, установленном законодательством Российской Федерации.

7. Уничтожение персональных данных

7.1. Документы, содержащие персональные данные, подлежат хранению и уничтожению в порядке, предусмотренном законодательством Российской Федерации.

7.2. Персональные данные работников подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в достижении таких целей.

7.3. Уничтожение документов, содержащих персональные данные, производится комиссионно. Комиссия назначается приказом заведующего РОО. По результатам работы комиссии оформляются акты об уничтожении.

8. Права субъектов персональных данных

Субъекты персональных данных имеют право на:

- полную информацию о своих персональных данных и обработке этих данных;
- свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законодательством;
- определение своих представителей для защиты своих персональных данных;
- требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением законодательства Российской Федерации;
- требование об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжалование в суд любых неправомерных действий или бездействия работодателя при обработке и защите своих персональных данных.

9. Ответственность работников при обработке персональных данных

9.1. Работники РОО при приеме на работу проходят инструктаж относительно принятых в РОО мер по защите персональных данных и порядке их обработки, после чего дают Согласие на обработку своих ПДн и Обязательство о неразглашении персональных данных и иной конфиденциальной информации (Приложение 6).

9.2. Разглашение персональных данных, то есть передача посторонним лицам, не имеющим к ним доступа; публичное раскрытие; утрата документов и иных носителей, содержащих персональные данные работника; иные нарушения обязанностей по их защите, обработке и хранению влекут наложение дисциплинарного взыскания - выговора, увольнения.

В случае причинения организации ущерба, связанного с нарушением правил обработки и защиты персональных данных работник несёт материальную ответственность в соответствии с п. 7 ч. 1 ст. 243 Трудового кодекса РФ.

В случае незаконного собирания или распространения работником сведений о частной жизни лица, составляющих его личную или семейную тайну, без согласия субъекта ПДн либо распространения этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации он несет уголовную ответственность.

9.3. Представление работником недостоверных сведений является основанием для вынесения дисциплинарных взысканий вплоть до увольнения, если данное действие не содержит состава преступления.

9.4. Положение обязательно для всех работников РОО.

9.5. В соответствии с требованиями п. 8 ст. 86 Трудового кодекса Российской Федерации, работники и их представители должны быть ознакомлены под роспись с документами работодателя, устанавливающими порядок обработки персональных данных, а также об их правах и обязанностях в этой области.

**Перечень персональных данных,
обрабатываемых в районном отделе образования
администрации Павинского муниципального района
в связи с реализацией трудовых отношений,
а также в связи с оказанием муниципальных услуг
и осуществлением муниципальных функций**

1. Перечень персональных данных, обрабатываемых в РОО, в связи с реализацией трудовых отношений:

- анкетные и биографические данные;
- образование;
- сведения о трудовом и общем стаже;
- паспортные данные;
- ИНН;
- номер страхового свидетельства государственного пенсионного страхования;
- сведения о воинском учете;
- сведения о заработной плате сотрудника;
- сведения о социальных льготах;
- специальность,
- занимаемая должность;
- адрес места жительства (по паспорту и фактический);
- домашний и мобильный телефон;
- характер взаимоотношений в семье;
- состояние здоровья
- содержание трудового договора;
- состав декларируемых сведений о наличии материальных ценностей;
- содержание декларации, подаваемой в налоговую инспекцию;
- подлинники и копии приказов по личному составу;
- личные дела и трудовые книжки сотрудников;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
- копии отчетов, направляемые в органы статистики.

2. Перечень персональных данных, обрабатываемых в РОО, в связи с оказанием муниципальных услуг и осуществлением муниципальных функций:

- фамилия, имя, отчество
- паспортные данные
- дата рождения
- адрес места жительства (по паспорту и фактический)
- контактный телефон
- номер страхового свидетельства государственного пенсионного страхования
- № и серия свидетельства о рождении ребенка;
- № и серия медицинского полиса
- состояние здоровья
- сведения о социальных льготах
- социальное положение семьи.

**Перечень должностей РОО
администрации Павинского муниципального района, замещение которых
предусматривает осуществление обработки персональных данных либо
осуществление доступа к персональным данным**

1. Заведующий районным отделом образования;
2. Заместитель заведующего районным отделом образования;
3. Ведущие специалисты-эксперты районного отдела образования;

СОГЛАСИЕ

на обработку персональных данных.

Я, _____, паспорт № _____, выдан _____ года
 _____, проживающий(ая) по адресу:
 _____ даю своё согласие районному отделу

образования администрации Павинского муниципального района расположенному по адресу: Костромская область, с. Павино, ул. Октябрьская, д.15, (далее Оператор) на обработку (автоматизированную и без использования средств автоматизации) моих персональных данных в целях соблюдения моих конституционных прав (ст. 24 Конституции РФ), исполнения требований федеральных законов, регулирующих работу с персональными данными (Трудовой и Налоговый Кодексы РФ, федеральный закон № 152-ФЗ «О защите персональных данных», иные нормативные акты), в целях содействия мне в обеспечении трудовой деятельности и установленных законодательством условий работы (гарантий и компенсаций), обеспечения моей личной безопасности, обучении и должностном росте, осуществления контроля количества и качества выполняемой работы, а также в целях систематизации производственной деятельности, организации функционального взаимодействия между подразделениями и обеспечения сохранности имущества Оператора, а именно:

- использовать нижеперечисленные данные для формирования кадровых документов и для выполнения Оператором всех требований трудового, налогового, страхового, пенсионного и иного федерального законодательства;

- использовать персональные данные в информационной системе персональных данных Оператора для ведения бухгалтерского учёта, осуществления расчетов Оператора со мной как работником;

Мои персональные данные, в отношении которых дается согласие, включают в себя:

- Фамилию, имя, отчество;
- Место и дату рождения;
- Паспортные данные (серия, номер паспорта, кем и когда выдан, место регистрации);
- Сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки (серия, номер, дата выдачи диплома, свидетельства, аттестата или другого документа об окончании образовательного учреждения, дата начала и завершения обучения, квалификация и специальность, данные о повышении квалификации или переподготовки);
- Сведения о трудовой деятельности (номер, серия, дата выдачи трудовой книжки и вкладышей к ней, данные о записях в трудовой книжке, должностной инструкции, приказах по л/составу, материалах аттестации и оценке трудовой деятельности, об имеющихся государственных и ведомственных наградах и т.п.);
- Сведения о семейном положении;
- Сведения о заработной плате;
- Сведения о воинском учёте военнообязанных лиц (номер военного билета, кем и когда выдан, иные данные);
- Сведения необходимые для определения социального статуса и предоставления социальных льгот (серия, номер, дата выдачи и наименование органа, выдавшего документы, являющиеся основанием для предоставления льгот);
- Сведения о страховом свидетельстве пенсионного страхования (номер СНИЛС);
- Сведения о регистрации в налоговом органе (ИНН);
- Контактные данные (телефонный номер: домашний, мобильный, E-mail);
- Место и адрес проживания;
- Сведения об изображении лица.

Данное согласие вступает в силу со дня его подписания и действует в течение периода моей работы. После моего увольнения Оператор обязан уничтожить мои персональные данные установленным порядком за исключением тех, хранение которых предусмотрено законодательством. Данное согласие может быть отозвано мною в любое время на основании моего письменного заявления.

 (дата)

 (подпись)

Типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные

Уважаемый (-ая), _____!
(инициалы субъекта персональных данных)

В соответствии с требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» уведомляем Вас, что обязанность предоставления Вами персональных данных установлена

(реквизиты и наименование нормативных правовых актов)

В случае отказа Вами предоставить свои персональные данные, оператор не сможет на законных основаниях осуществлять такую обработку, что приведет к следующим для Вас юридическим последствиям _____

(перечисляются юридические последствия для субъекта персональных данных, то есть случаи возникновения, изменения или прекращения личных либо имущественных прав граждан или случаи иным образом затрагивающие его права, свободы и законные интересы)

В соответствии с законодательством в области персональных данных Вы имеете право:

на получение сведений об операторе, о месте его нахождения, о наличии у оператора своих персональных данных, а также на ознакомление с такими персональными данными;

требовать уточнения своих 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;

на получение при обращении или при направлении запроса информации, касающейся обработки своих персональных данных;

на обжалование действия или бездействия оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке; на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

(дата)

(фамилия, инициалы и подпись сотрудника оператора)

Наименование (Ф.И.О.) оператора

Адрес оператора

Ф.И.О. субъекта персональных данных

Адрес, где зарегистрирован субъект персональных данных

Номер основного документа, удостоверяющего личность

Дата выдачи указанного документа

Наименование органа, выдавшего документ

ЗАЯВЛЕНИЕ

На основании п. 2 ст. 9 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», отзываю ранее данное мной согласие на обработку персональных данных.

В случае, если согласие на обработку персональных данных давалось мной неоднократно, настоящим я отзываю все ранее данные мной согласия на обработку персональных данных.

В соответствии с п. 5 ст. 21 Федерального закона «О персональных данных», в случае отзыва субъектом персональных данных согласия на их обработку, оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва.

Я уведомлен, что в случае отзыва согласия на обработку персональных данных, районный отдел образования администрации Павинского муниципального района вправе продолжить обработку персональных данных без моего согласия при наличии оснований, указанных в пунктах 2-41 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»

Уведомление о прекращении обработки и уничтожении моих персональных данных прошу предоставить в письменной форме.

« ____ » _____ 20 ____ г

_____/_____
(подпись) (расшифровка подписи)

ОБЯЗАТЕЛЬСТВО
о неразглашении персональных данных и иной конфиденциальной информации

Я, _____,

уведомлен(а), что в процессе работы в районном отделе образования администрации Павинского муниципального района получу доступ к конфиденциальной информации, в том числе, к отдельным категориям персональных данных сотрудников РОО, должностных лиц подведомственных образовательных учреждений и контрагентов, граждан РФ, обратившихся в РОО.

Я подтверждаю, что ознакомлен(а) с Положением об обработке персональных данных и иными нормативными документами, определяющими порядок обработки (сбор, запись, систематизацию, накопление, хранение, уточнение, извлечение, использование, передачу, обезличивание, блокирование, удаление, уничтожение) и защиты сведений, относимых к конфиденциальной информации.

Я подтверждаю, что не имею никаких обязательств перед каким-либо третьим лицом (физическим или юридическим), которые входят в противоречие с настоящим Обязательством, и обязуюсь в период трудовых отношений с РОО и после их окончания:

- не разглашать и не передавать третьим лицам информацию, содержащую персональные данные, а также иные конфиденциальные сведения, которые мне будут доверены или станут известны при выполнении моих трудовых обязанностей;
- выполнять требования локальных нормативных актов и руководящих документов по обеспечению защиты информации в части меня касающейся;
- сообщать непосредственному руководителю о случаях попытки посторонних лиц получить от меня защищаемые сведения;
- сохранять ставшую мне известной в связи с выполнении моих трудовых обязанностей конфиденциальную информацию;
- сообщать непосредственному руководителю о фактах утраты или обнаружении недостачи материальных носителей конфиденциальной информации, а также утраты иных атрибутов (ключей от хранилищ, сейфов и т.п.), которые могут привести к разглашению или утечке защищаемой информации;
- в случае моего увольнения передать непосредственному руководителю все имеющиеся материальные носители конфиденциальной информации, находящиеся в моём распоряжении в связи с исполнением с выполнением моих трудовых обязанностей, на которых хранится или может храниться конфиденциальная информация. Мне известно, что в случае невыполнения мной любого из вышеперечисленных пунктов настоящего Обязательства в отношении меня могут быть применены меры ответственности, предусмотренные трудовым, административным и уголовным законодательством Российской Федерации, включая обязанность по возмещению всех причиненных убытков.

Работник

(подпись)

(фамилия, имя, отчество)

« ____ » _____ 20 ____ г.

**Правила
рассмотрения запросов субъектов персональных данных
или их представителей в районном отделе образования
администрации Павинского муниципального района**

1. Настоящими Правилами рассмотрения запросов субъектов персональных данных или их представителей в районном отделе образования администрации Павинского муниципального района (РОО) (далее - Правила) определяется порядок учета (регистрации) и рассмотрения запросов субъектов персональных данных или их представителей (далее - запросы).

2. Настоящие Правила разработаны в соответствии с Федеральным законом от 27 июля 2006 года N 152-ФЗ "О персональных данных" (далее - Федеральный закон N 152-ФЗ), Федеральным законом от 2 мая 2006 года N 59-ФЗ "О порядке рассмотрения обращений граждан Российской Федерации", Федеральным законом от 2 марта 2007 года N 25-ФЗ "О муниципальной службе в Российской Федерации", Трудовым кодексом Российской Федерации, Постановлением Правительства Российской Федерации от 15 сентября 2008 года N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации" и другими нормативными правовыми актами.

3. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных в РОО;
- правовые основания и цели обработки персональных данных;
- цели и применяемые в РОО способы обработки персональных данных;
- наименование и место нахождения оператора (РОО), сведения о лицах (за исключением работников РОО), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
- 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;
- порядок осуществления субъектом персональных данных прав, предусмотренных настоящими Правилами;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные федеральными законами.

4. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с частью 8 статьи 14 Федерального закона N 152-ФЗ.

5. Субъект персональных данных вправе требовать от уполномоченных должностных лиц Отдела образования уточнения его 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.

6. Сведения, указанные в пункте 3 настоящих Правил, предоставляются субъекту персональных данных или его представителю при направлении запроса субъекта

персональных данных или его представителя в РОО.

7. Сведения, указанные в пункте 3 настоящих Правил, должны быть предоставлены субъекту персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

8. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с РОО (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных РОО, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации (Приложение 1).

9. Рассмотрение запросов является служебной обязанностью заведующего и уполномоченных должностных лиц РОО, в чьи обязанности входит обработка персональных данных.

10. Уполномоченные должностные лица РОО обеспечивают:

- объективное, всестороннее и своевременное рассмотрение запроса;
- принятие мер, направленных на восстановление или защиту нарушенных прав, свобод и законных интересов субъектов персональных данных;
- направление письменных ответов по существу запроса.

11. Ведение делопроизводства по запросам субъектов персональных данных или их представителей осуществляется специально назначенным работником РОО.

12. Все поступившие запросы регистрируются в день их поступления в Журнале регистрации запросов субъектов персональных данных или их представителей. (Приложение 2). На запросе проставляется штамп, в котором указывается входящий номер и дата регистрации.

13. Запрос прочитывается, проверяется на повторность, при необходимости сверяется с находящейся в архиве предыдущей перепиской.

14. В случае если сведения, указанные в пункте 3 настоящих Правил, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в РОО или направить повторный запрос в целях получения сведений, указанных в пункте 3 настоящих Правил, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

15. Субъект персональных данных вправе обратиться повторно в РОО или направить повторный запрос в целях получения сведений, указанных в пункте 3 настоящих Правил, а также в целях ознакомления с обрабатываемыми персональными данными, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду с необходимыми сведениями должен содержать обоснование направления повторного запроса.

16. РОО вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным частями 4 и 5 статьи 14 Федерального закона N 152-ФЗ, с указанием оснований для такого отказа.

17. Прошедшие регистрацию запросы в тот же день направляются заведующему РОО

либо лицу, его заменяющему, который определяет порядок и сроки их рассмотрения, дает по каждому из них письменное указание исполнителям.

18. Заведующий РОО и другие должностные лица при рассмотрении и разрешении запроса обязаны:

- разобраться в существе запроса, в случае необходимости истребовать дополнительные материалы или осуществить проверку фактов, изложенных в запросах, принять другие меры для объективного разрешения поставленных заявителями вопросов, выявления и устранения причин и условий, порождающих факты нарушения законодательства о персональных данных;

- принимать законные, обоснованные и мотивированные решения и обеспечивать своевременное и качественное их исполнение;

- сообщать в письменной форме заявителям о решениях, принятых по их запросам, со ссылками на законодательство Российской Федерации, а в случае отклонения запроса - разъяснять также порядок обжалования принятого решения.

19. В ответе РОО сообщается информация о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставляется возможность ознакомления с этими персональными данными при личном обращении субъекта персональных данных или его представителя в течении тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

20. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя уполномоченные должностные лица РОО обязаны дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона N 152-ФЗ или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

21. Возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных, предоставляется субъекту персональных данных или его представителю бесплатно.

22. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, уполномоченные должностные лица РОО обязаны внести в них необходимые изменения.

23. Уполномоченные должностные лица РОО обязаны уведомить субъект персональных данных или его представителя о внесенных изменениях и принять меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

24. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, уполномоченные должностные лица РОО обязаны уничтожить такие персональные данные.

25. В случае поступления сведений о неправомерной обработке персональных данных при обращении либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных уполномоченные должностные лица РОО обязаны осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения указанного запроса на период проверки.

26. В случае выявления неправомерной обработки персональных данных

уполномоченные должностные лица РОО в срок, не превышающий трех рабочих дней с даты этого выявления, обязаны прекратить неправомерную обработку персональных данных. В случае, если обеспечить правомерность обработки персональных данных невозможно, уполномоченные должностные лица РОО в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязаны уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных РОО обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также уведомляется указанный орган.

27. В случае выявления неточных персональных данных при обращении либо по запросу субъекта персональных данных или его представителя, или по запросу уполномоченного органа по защите прав субъектов персональных данных уполномоченные должностные лица РОО обязаны осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

28. В случае подтверждения факта неточности персональных данных уполномоченные должностные лица РОО на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов, обязаны уточнить персональные данные в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

29. При необходимости для проверки фактов, изложенных в запросах субъектов персональных данных или их представителей, в РОО организуются служебные проверки в соответствии с законодательством Российской Федерации.

30. По результатам служебной проверки составляется мотивированное заключение, которое должно содержать объективный анализ собранных материалов. Если при проверке выявлены факты совершения должностным лицом РОО действия (бездействия), содержащего признаки административного правонарушения или состава преступления, информация передается в правоохранительные органы. Результаты служебной проверки докладываются заведующему РОО.

31. Запрос считается исполненным, если рассмотрены все поставленные в нем вопросы, приняты необходимые меры и даны исчерпывающие ответы заявителю.

32. Ответы на запросы печатаются на бланке установленной формы и регистрируются за теми же номерами, что и запросы.

33. Контроль за соблюдением установленного законодательством и настоящими Правилами порядка рассмотрения запросов осуществляется заведующим РОО.

34. Заведующий РОО осуществляет контроль за работой с запросами и организацией их приема, так и через своих работников. На контроль берутся все запросы.

34. При осуществлении контроля обращается внимание на сроки исполнения поручений по запросам и полноту рассмотрения поставленных вопросов, объективность проверки фактов, изложенных в запросах, законность и обоснованность принятых по ним решений, своевременность их исполнения и направления ответов заявителям.

35. Нарушение установленного порядка рассмотрения запросов влечет в отношении виновных должностных лиц РОО ответственность в соответствии с законодательством Российской Федерации.

Приложение 1
к правилам рассмотрения запросов
субъектов персональных данных
или их представителей в РОО

**Форма запроса на предоставление информации,
касающейся обработки персональных данных
субъекта персональных данных**

_____ (наименование или Ф.И.О. оператора)
от _____ (Ф.И.О. субъекта персональных данных)
адрес: _____
телефон: _____, факс _____
электронный адрес: _____

ЗАПРОС

В период с " ____ " _____ г. по " ____ " _____ г.
обработывались следующие персональные данные:

_____ (перечень обрабатываемых персональных данных)
С _____ целью

_____ (цель обработки персональных данных)
в форме _____
_____ (способы обработки персональных данных)
субъекта персональных данных - _____

_____ (Ф.И.О., паспортные данные, в том числе дата выдачи, выдавший орган)
оператором - _____

_____ (наименование или Ф.И.О. оператора, ИНН, адрес)
Обработка проводилась в рамках _____

_____ (номер, дата договора либо сведения, иным образом подтверждающие факт обработки персональных данных оператором)
В связи с _____

_____ (обоснование причин)
и на основании частей 3 и 7 статьи 14, статьи 18, части 1 статьи 20
Федерального закона от 27 июля 2006 года N 152-ФЗ "О персональных данных"
прошу предоставить следующую информацию, касающуюся обработки указанных
персональных _____ данных:

_____ (существо запроса)
_____ ,
в следующем порядке _____ в срок до _____ .

" ____ " _____ года

Субъект персональных данных _____ (подпись) _____ (ФИО)

Приложение 2
к правилам рассмотрения запросов
субъектов персональных данных
или их представителей в РОО

ЖУРНАЛ
регистрации запросов субъектов персональных данных
или их представителей

Начат «____» _____ 20____ г.
Окончен «____» _____ 20____ г.

№ п/п	ФИО субъекта	Дата обращения	Содержание запроса	Отметка об исполнении	ФИО исполнителя	Подпись

**Правила работы с обезличенными
персональными данными, обрабатываемыми
в районном отделе образования администрации Павинского муниципального района**

1. Настоящие Правила работы с обезличенными персональными данными, обрабатываемыми в районном отделе образования администрации Павинского муниципального района (РОО) (далее - Правила), разработаны в соответствии с Федеральным законом от 27 июля 2006 года N 152-ФЗ "О персональных данных", Постановлением Правительства Российской Федерации от 15 сентября 2008 года N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации" и определяют порядок работы с обезличенными персональными данными в РОО.

2. В настоящих Правилах используются термины и определения, установленные Федеральным законом от 27 июля 2006 года N 152-ФЗ "О персональных данных".

3. Обезличивание персональных данных в РОО проводится с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижение класса информационных систем персональных данных.

4. Способами обезличивания персональных данных при условии их дальнейшей обработки являются:

- а) уменьшение перечня обрабатываемых сведений;
- б) замена части сведений идентификаторами;
- в) обобщение - понижение точности некоторых сведений;
- г) понижение точности некоторых сведений (например, "Место жительства" может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только город);
- д) деление сведений на части и обработка в разных информационных системах;
- е) иные способы.

5. Способом обезличивания персональных данных в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.

6. Для обезличивания персональных данных годятся любые способы явно не запрещенные законодательно.

7. Заведующий РОО принимает решение о необходимости обезличивания персональных данных.

8. Работники РОО, непосредственно осуществляющие обработку персональных данных, готовят предложения по обезличиванию персональных данных, обоснование такой необходимости и способ обезличивания.

9. Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

10. Обезличенные персональные данные обрабатываются с использованием и без использования автоматизации.

11. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:

- а) парольной политики;
- б) антивирусной политики;
- в) правил работы со съемными носителями (если они используются);
- г) правил резервного копирования;
- д) правил доступа в помещения, где расположены элементы информационных систем.

12. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

- а) правил хранения бумажных носителей;
- б) правил доступа к ним и в помещения, где они хранятся.

**Правила
осуществления внутреннего контроля соответствия обработки персональных
данных требованиям нормативных документов**

1. Общие положения

1.1. Настоящие Правила разработаны на основании требований пункта 4 части 1 ст. 18.1 и пункта 1 части 4 ст. 22.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и п. 6 ст. 1 Постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных».

1.2. В соответствии с законодательством Оператор ПДн обязан осуществлять внутренний контроль принятых мер, необходимых и достаточных для обеспечения безопасной обработки персональных данных и иной конфиденциальной информации, обрабатываемой в организации.

1.3. Оператор ПДн самостоятельно с учётом штатной структуры РОО, установленного порядка обработки персональных данных (их сбора, хранения, модификации, передачи, распространения и уничтожения), а также параметров автоматизированной информационной системы, в которой обрабатывается конфиденциальная информация, определяет состав и перечень режимных, правовых и технических мер для обеспечения её защиты.

1.4. Мероприятия по осуществлению внутреннего контроля проводятся на плановой основе в соответствии с утверждаемыми заведующим РОО ежегодными планами.

2. Основные направления внутреннего контроля

В соответствии с требованиями федерального законодательства, регулирующего сферу обработки персональных данных и иной конфиденциальной информации регулярному контролю подвергаются:

2.1. Исполнение требований обработки персональных данных, установленных внутренними нормативными документами (Правилами, Положениями, Инструкциями, Порядками).

2.2. Контроль соответствия категорий персональных данных, обрабатываемых в РОО, заявленным в Перечне персональных данных утвержденном актом руководителя.

2.3. Соответствие должностей работников, замещение которых предусматривает обработку персональных данных, заявленному в утвержденном актом заведующего РОО Перечне должностей.

2.4. Выполнение порядка допуска работников РОО к обработке персональных данных и иной конфиденциальной информации с использованием средств автоматизации и без использования таковых.

2.5. Выполнение работниками РОО требований по обеспечению безопасного хранения материальных и электронных носителей персональных данных и доступа к ним посторонних лиц.

2.6. Реализация исполнения требований учётной политики при работе с материальными и электронными носителями.

2.7. Выполнение установленных режимных требований, правил доступа к местам хранения и обработки конфиденциальной информации, в том числе персональных данных.

2.8. Соответствие требований принятых для ИСПДн мер технической защиты требованиям, предусмотренным приказом ФСТЭК РФ от 18.02.2013 г. № 21, в соответствии с актуальными угрозами и определённым уровнем защищенности персональных данных.

2.9. Исполнение порядка ознакомления работников РОО с нормативными документами, регламентирующими безопасную обработку персональных данных;

2.10. Выполнение порядка и сроков обработки поступающих в РОО запросов от субъектов ПДн.

2.11. Проверка соответствия условий и режима обработки персональных данных, внесенных в реестр Операторов ПДн, действительному положению. Внесение, при необходимости, изменений в направленное ранее Уведомление об обработке ПДн.

3. Порядок осуществления контроля

3.1. Осуществление мероприятий внутреннего контроля проводится строго в соответствии с установленными в Плане сроками и обязательной отметкой о выполненном мероприятии.

3.2. Контрольные проверки могут осуществляться лицом, ответственным за организацию обработки персональных данных самостоятельно либо с привлечением должностных лиц, имеющих допуск к обработке персональных данных в соответствии с профилем проводимого мероприятия.

3.3. При необходимости по распоряжению руководства организации могут проводиться внеплановые проверки по различным направлениям порядка обработки и защиты персональных данных.

3.4. За нарушение требований действующего законодательства, виновные несут ответственность в соответствии со ст. 24 Федерального закона от 27.07.2006 г. № 152 ФЗ «О персональных данных».

**Правила
работы с информационными системами районного отдела образования
администрации Павинского муниципального района**

1. Общие положения

1.1. Настоящие Правила определяют основные принципы безопасной работы автоматизированных информационных систем РОО и обработки конфиденциальной информации сотрудниками РОО (Приложение 1.)

1.2. Целью данного документа является формализация требований, предъявляемых к сотрудникам, по обеспечению режима безопасности конфиденциальной информации, циркулирующей в информационных системах, в том числе при обработке персональных данных.

1.3. Правила разработаны в соответствии с требованиями Федеральных законов РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 № 152-ФЗ «О персональных данных», постановлений Правительства РФ от 01.11.2012 № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных», от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и иных нормативных актов.

2. Основные термины и определения

Автоматизированное рабочее место пользователя (далее АРМ) - персональный компьютер с предустановленным системным, прикладным и антивирусным программным обеспечением (далее ПО), в том числе предназначенным для защиты информации ограниченного распространения.

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

Информационные ресурсы - программное обеспечение, документы и массивы документов расположенные, хранящиеся и обрабатываемые в информационных системах;

Интернет - всемирная система объединённых компьютерных сетей, построенная на использовании протокола IP и маршрутизации пакетов данных (телекоммуникационная сеть общего пользования);

Пользователь - сотрудник, допущенный к работе на автоматизированном рабочем месте и использующий для исполнения своих должностных обязанностей средства вычислительной техники;

Персональный компьютер (далее ПК) - компьютер, с предустановленным системным, прикладным и антивирусным ПО и предназначенный для эксплуатации одним пользователем, то есть для личного использования;

Электронная почта - технология и предоставляемые ею услуги по пересылке и получению электронных сообщений (называемых «письма» или «электронные письма») по распределённой (в том числе глобальной) компьютерной сети;

Flash-карта - разновидность твердотельной полупроводниковой энергонезависимой перезаписываемой памяти (один из видов электронных носителей информации).

3. Общие правила работы на АРМ

3.1. В целях исполнения своих служебных обязанностей, сотруднику РОО (пользователю) на период работы предоставляется автоматизированное рабочее место с предустановленным лицензионным системным, прикладным и антивирусным программным обеспечением, имеющим сертификаты соответствия по безопасности.

Для организации доступа пользователя к информационным ресурсам АИС его АРМ подключается к локальной вычислительной сети (далее ЛВС).

3.2. Допуск пользователя к АРМ осуществляется по устной заявке заведующего РОО (либо его заместителя) на основании утвержденного Перечня должностей, имеющих право доступа к обработке конфиденциальной информации, в том числе персональных данных.

Доступ пользователя к работе на АРМ осуществляется на основании индивидуальной учетной записи (Логин + Пароль). Пользователь обязан использовать пароль в соответствии со следующими требованиями:

- длина пароля должна быть не менее 8 символов;
- пароль должен состоять из строчных и прописных букв, а также небуквенных символов (т.е. цифр, знаков пунктуации, специальных символов);
- пароль не должен быть легко угадываемым (не должен включать повторяющуюся последовательность каких-либо символов (например, "11111111", "абвгдеё" и т.п.), пароль не должен включать в себя легко подбираемые сочетания символов (имена, фамилии, даты рождения знакомых, наименования городов и улиц, клички домашних животных и т.п.), а также общепринятые сокращения (ЭВМ, ЛВС и т.п.).

3.3. Пользователь обеспечивает безопасное хранение пароля, исключая возможность его утери или разглашения. Срок использования пароля составляет не более 90 дней. При смене пароля новое значение должно отличаться от предыдущего не менее чем в трёх-четырёх позициях.

3.4. При необходимости оставить рабочее место, даже на короткое время, пользователь должен заблокировать доступ к АРМ, нажав одновременно Ctrl + Alt + Delete, и принять иные меры по ограничению доступа к отображаемой на экране монитора информации

3.5. При использовании телекоммуникационных возможностей сети общего пользования Интернет пользователи обязаны выполнять следующие требования:

- использовать ресурсы Интернет только для выполнения своих служебных обязанностей;
- не посещать ресурсы Интернет, содержащие материалы противозаконного, экстремистского или неэтичного характера, а также использовать доступ к социальным сетям Интернет и развлекательным сайтам;
- не размещать в сети Интернет информацию служебного характера, о её сотрудниках и решаемых задачах, если это не связано с выполнением служебных обязанностей; - не использовать Интернет для несанкционированной передачи (выгрузки) или получения (загрузки) видео-, аудио- и информационных материалов, защищенных авторским правом;

3.6. При работе с электронной почтой пользователи должны соблюдать следующие требования:

- запрещается использовать возможности электронной почты для отправки сообщений противозаконного (террористического, экстремистского или враждебного характера), а также содержащего в себе информацию неэтичного содержания;
- при получении электронных сообщений из незнакомого источника и/или сомнительного содержания не следует открывать файлы, вложенные в сообщение, так как они с большой долей вероятности могут содержать вирусы. Такие сообщения необходимо удалять;
- не отвечать на подозрительные письма и, тем более, сообщать любые данные о себе и сотрудниках.

3.7. По окончании рабочего времени при отсутствии служебной необходимости пользователь обесточивает АРМ и другую оргтехнику во избежание выхода её из строя и в целях обеспечения противопожарной безопасности.

3.8. В случае подозрения на компрометацию пароля доступа необходимо немедленно изменить пароль и проинформировать об этом своего непосредственного руководителя.

В процессе эксплуатации АРМ пользователям ЗАПРЕЩАЕТСЯ:

3.9. Открывать корпус системного блока и вносить изменения в конфигурацию ПК;

3.10. Без получения санкции руководителя и администратора безопасности изменять настройки программного обеспечения и параметры доступа к информационным ресурсам;

3.11. Отключать и изменять параметры настройки в установленное антивирусное программное обеспечение и иные средства защиты информации;

3.12. Подключать к АРМ неучтенные внешние запоминающие устройства (активное сетевое оборудование, незарегистрированные Flash-карты, НЖМД, смартфоны, фотоаппараты и т.д.), если это не связано с исполнением должностных обязанностей сотрудника;

3.13. Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты для организации несанкционированного доступа к обрабатываемым информационным ресурсам. При обнаружении такого рода ошибок необходимо информировать своего непосредственного руководителя и администратора безопасности;

3.14. Осуществлять действия направленные на преодоление систем безопасности, получение несанкционированного доступа к ресурсам информационной сети и перехват информации, циркулирующей в ИС;

3.15. Оставлять оборудование АРМ, переносные компьютеры и средства хранения информации без личного присмотра, в случаях, если это может привести к их краже;

При наличии риска хищения ПК и (или) средств хранения информации, необходимо принять меры по их минимизации (например, убирать переносной компьютер на обеденный перерыв и после завершения рабочего дня в закрывающийся на ключ шкаф, не оставлять незакрытым помещение, в котором находится оборудование информационной системы, использовать замки для переносных компьютеров);

3.16. Осуществлять обработку конфиденциальной информации на ПК, не оснащенных принятыми в РОО средствами защиты информации, а также в присутствии

лиц, не имеющих права доступа к данной информации, если при этом указанные лица могут ознакомиться с обрабатываемой информацией;

3.17. Записывать и хранить конфиденциальную информацию на неучтённых носителях информации (Flash-карта, CD-диск, носимый HDD и т.п), а также оставлять без личного присмотра на рабочем месте или где бы то ни было носители информации и распечатки, содержащие подобную информацию;

3.18. Допускать к работе на ПК лиц, не имеющих прав доступа к информационным ресурсам.

4. Порядок работы с информационной системой

4.1. При работе с программными и техническими средствами, входящими в состав АРМ и информационной системы, пользователь обязан выполнять установленные правила их эксплуатации. За неисполнение установленных правил он несёт персональную ответственность.

4.2. РОО оставляет за собой право протоколировать и контролировать действия сотрудников при обработке конфиденциальной информации обрабатываемой в информационной системе.

4.3. Пользователи не имеют права предпринимать попыток получения доступа к закрытым информационным ресурсам, не получив официального разрешения на доступ к ним.

4.4. Пользователи не должны разглашать сведения о содержании информации, ставшей известной им в ходе выполнения должностных обязанностей, а также о процедурах и технической реализации защиты информации, принятых в департаменте.

4.5. В целях повышения эффективности служебной деятельности для обмена открытыми информационными ресурсами (обновления программных продуктов, инструкции, правила и т.п.) между пользователями могут использоваться съёмные материальные носители информации (Flash-карты, переносные жесткие диски, иные устройства записи и чтения), зарегистрированные и учтённые по Журналу учёта съёмных носителей информации.

4.6. Выдача сотрудникам и учёт материальных носителей информации осуществляется сотрудником, ответственным за организацию работы по защите персональных данных, по Журналу учёта съёмных носителей информации.

5. Ответственность за нарушение порядка

5.1. Ответственность за неисполнение требований настоящей Инструкции возлагается на всех сотрудников, являющихся пользователями информационной системы департамента.

5.2. Сотрудник, нарушивший требования данной Инструкции, может быть подвергнут дисциплинарному наказанию в соответствии с законодательством Российской Федерации (уголовный, налоговый, гражданский, трудовой Кодексы и иное законодательство).

**Инструкция
по проведению антивирусного контроля на автоматизированном рабочем
месте (АРМ)**

1. Настоящая Инструкция предназначена для пользователей, обрабатывающих персональные данные с использованием средств автоматизации.
2. В целях обеспечения защиты автоматизированной информационной системы от программных закладок и программно-математического воздействия на обрабатываемые конфиденциальные данные на автоматизированных рабочих местах (АРМ) производится антивирусный контроль.
3. На АРМ пользователя запрещается установка прикладного программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации на АРМ.
4. Пользователи АРМ при работе с информацией (ПО, БД, файлы) записанной на электронных носителях информации (Flash-карты, CD-диски, дискеты и т.п.) обязаны перед началом работы осуществить их проверку на предмет отсутствия компьютерных вирусов.
5. Ярлык для запуска антивирусной программы должен быть вынесен на "Рабочий стол" операционной системы.
6. Обновление вирусных баз осуществляется ежедневно путём скачивания и установки антивирусных баз с сервера производителя антивирусного ПО.
7. При обнаружении компьютерного вируса в процессе эксплуатации АРМ либо сканирования съёмных электронных носителей информации пользователь обязан немедленно поставить об этом в известность администратора безопасности и прекратить какие-либо действия, связанные с обработкой конфиденциальной информации на АРМ.
8. По факту заражения АРМ компьютерным вирусом производится «лечение» зараженных файлов путём выбора соответствующего пункта меню антивирусной программы, после чего вновь проводит антивирусный контроль файловой системы и обрабатываемых данных на АРМ.
12. О всех фактах заражения АИС и АРМ вредоносным программным обеспечением необходимо проинформировать заведующего РОО.

**Инструкция
по резервному копированию информации и восстановлению
работоспособности ИС**

1. Общие положения.

1.1. В целях предупреждения возможности неблагоприятных последствий и обеспечения защиты важной или критичной для обеспечения работоспособности автоматизированных информационных систем информации от её случайного либо умышленного уничтожения, модификации или хищения, а также обеспечения её сохранности необходимо создавать её резервные копии.

1.2. Настоящая Инструкция разработана в соответствии с требованиями Федеральных законов от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации» и от 27.07.2006 № 152-ФЗ «О персональных данных», постановлений Правительства РФ от 15.09.2008 № 687 «Об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и от 01.11.2012 № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных» и иных нормативных документов и определяет общие правила резервирования обрабатываемых данных, в том числе при обработке информации ограниченного распространения (обработка персональных данных и иной конфиденциальной информации).

1.3. При осуществлении резервирования (резервного копирования) данных пользователи в своей работе руководствуются настоящей Инструкцией, иными внутренними нормативными документами и требованиями законодательства в сфере защиты информации ограниченного доступа.

1.4. Резервирование данных проводится для обеспечения восстановления работоспособности автоматизированных информационных систем (АИС), вызванной сбоем в работе либо отказами аппаратного и программного обеспечения, чрезвычайными обстоятельствами, ошибками пользователей и (или) иными внешними воздействиями, ведущими к полной или частичной утрате информации.

1.5. Требования настоящей Инструкции, связанные с резервным копированием критичной информации обязательны для исполнения всеми сотрудниками (пользователями), обрабатывающими такую информацию.

2. Термины и определения

Автоматизированная информационная система (АИС) - взаимосвязанная совокупность данных, оборудования, программных средств, персонала, реализующая информационную технологию выполнения установленных функций, предназначенных для сбора, обработки, распределения, хранения, выдачи (предоставления) информации (по ГОСТ 34.003).

Критичная информация - любая важная информация, а также системное и прикладное программное обеспечение, утрата которых может привести к перебоям либо отказу в работе автоматизированной информационной системы и затруднению (либо невозможности) исполнения служебных обязанностей.

Резервное копирование - сохранение текущего состояния информации (системы) без обязательного сохранения предыдущего.

Съемный носитель информации - носитель информации, предназначенный для автономного хранения информации вне зависимости от места записи и использования (НЖМД, CD-DVD-диск, Flash-накопитель и т.п.).

Гарантированное хранение - хранение, обеспечивающее целостность информации, определяемую требованиями федерального законодательства и внутренними организационно-распорядительными документами Отдела образования.

3. Информация, подлежащая резервированию

В целях скорейшего восстановления работоспособности автоматизированной ИС и исключения неблагоприятных последствий вызванных отказами в её работе либо утратой критичной информации в РОО определен перечень информационных ресурсов, системного и прикладного ПО, подлежащих резервному копированию (Приложение 1), в который включен:

3.1. Персональные данные работников организации, обрабатываемые с использованием средств автоматизации и прикладного программного обеспечения в бухгалтерии.

3.2. Инсталляции системного и прикладного ПО, используемого для защиты и обработки критичной информации, персональных данных и иной конфиденциальной информации.

4. Порядок резервирования данных

Организация обеспечения резервного копирования обрабатываемой критичной информации, в том числе персональных данных, возложена на руководителей структурных подразделений РОО, в которых она обрабатывается (одного из его сотрудников).

4.1. Обязательному резервному копированию и гарантированному хранению подлежит информация, указанная в Приложении 1.

4.2. В качестве носителей, на которые осуществляется резервное копирование информации, в зависимости от сохраняемых информационных ресурсов, используются:

- папки на сетевом диске РОО;
- накопители на жестких магнитных носителях АРМ пользователей, физически разнесенные с накопителями, где происходит обработка критичной информации; - перезаписываемые или не перезаписываемые диски (CD, DVD, Blu-Ray).

4.3. К носителям, на которые производится резервное копирование предъявляются следующие требования:

4.4.1. Наличие достаточного объема свободного дискового пространства либо свободной памяти для обеспечения надежного хранения резервных копий;

4.4.2. Носитель должен периодически проходить полную проверку целостности (не реже одного раза в 6 месяцев);

4.4.3. Носитель должен быть учтён по Журналу учёта электронных носителей с указанием наименования, информационной емкости, ответственного за его эксплуатацию сотрудника;

4.4.4. К носителю должен быть ограничен физический доступ посторонних лиц, в том числе по сети. Его хранение осуществляется в местах с ограниченным доступом (запираемый шкаф, сейф и т.п.);

4.4.5. Ход выполнения установленных требований соблюдения установленных правил хранения и доступа, целостности ячеек памяти и работоспособности осуществляется на регулярной основе в соответствии с планом проведения внутренних проверок.

4.5. Период сохранения резервных копий определяется комиссионно, исходя из целесообразности обеспечения гарантированного сохранения тех или иных информационных ресурсов (частота внесения изменений в данные, критичность их утраты и т.п.) и производится по окончании рабочего времени ежеквартально, ежегодно с сохранением информации за указанный период + 1 день.

5. Порядок восстановления работоспособности ИС

5.1. В случае потери (уничтожения, модификации) критичной информации пользователь информационных ресурсов ИСПДн либо ответственный работник обязан сообщить заведующему РОО о факте произошедшего сбоя в работе информационной системы, в результате которого произошла утрата данных. При этом сотрудник сообщает о возможных признаках сопутствующих отказу в работе АИС и принимает незамедлительные меры по восстановлению утраченной информации в кратчайший срок.

5.2. При потере критичной информации хранящейся на сетевом диске локальной информационной системы восстановление производится при участии заведующего РОО.

5.3. По итогам произошедшего инцидента с утратой критичной информации в целях предотвращения подобных фактов в дальнейшем заведующим РОО проводится разбирательство с выявлением причин инцидента и лиц, допустивших нарушение.

6. Ответственность за нарушение установленного порядка резервирования данных

6.1. Персональная ответственность за обеспечение безопасного хранения критичной информации пользователя в соответствии с установленным порядком возлагается на ответственных работников, обрабатывающих эту информацию.

6.2. Ответственность за обеспечение резервного копирования критичной информации, обрабатываемой и сохраняемой в ИСПДн, возлагается на руководителя и ответственных работников подразделений.

6.3. Хранение резервных копий и инсталляций эксплуатируемого ПО, серийных номеров и регистрационных кодов возлагается на администратора безопасности.

6.4. Нарушение требований настоящей Инструкции влечёт за собой дисциплинарную ответственность в соответствии с трудовым законодательством РФ.

6.5. К лицам, нарушившим установленный порядок резервирования критичной информации, обеспечения сохранности и уничтожения электронных носителей информации ограниченного доступа, вследствие которых произошло нанесение материального ущерба организации, могут быть приняты меры по возмещению убытков и компенсации морального вреда¹.

Приложение 1.
к инструкции по резервному
копированию информации и
восстановлению работоспособности ИС

ПЕРЕЧЕНЬ
критичных информационных ресурсов, подлежащих резервному копированию

№ п/п	Наименование информационного ресурса	Подразделение (сотрудник) ответственное за резервирование	Период резервирования	Носитель
1.	Системное ПО		При установке	DVD-диск
2.	Прикладное ПО		При установке	DVD-диск

**Типовая форма
журнала учета съемных носителей персональных данных**

Окончен " " 20 года

[illegible]

**Порядок
доступа в помещения районного отдела образования администрации
Павинского муниципального района,
в которых ведется обработка персональных данных**

1. Настоящий Порядок доступа в помещения, в которых ведется обработка персональных данных (далее - Порядок), устанавливает единые требования к доступу в служебные помещения в целях предотвращения нарушения прав субъектов персональных данных, обрабатываемых в районном отделе образования администрации Павинского муниципального района (далее - РОО), и обеспечения соблюдения требований законодательства о персональных данных.
2. Настоящий Порядок обязателен для применения и исполнения всеми работниками РОО.
3. Помещения, в которых ведется обработка персональных данных (Приложение), должны обеспечивать сохранность информации и технических средств, исключать возможность бесконтрольного проникновения в помещение и их визуального просмотра посторонними лицами и оснащены охранной сигнализацией
4. Персональные данные на бумажных носителях должны находиться в недоступном для посторонних лиц месте.
5. Бумажные носители персональных данных и электронные носители персональных данных (диски, флеш-карты) хранятся в металлических шкафах (сейф).
6. Помещения, в которых ведется обработка персональных данных, запираются на ключ.
7. Перед закрытием помещений, в которых ведется обработка персональных данных, по окончании рабочего времени работники, имеющие право доступа в помещения, обязаны:
 - убрать бумажные носители персональных данных и электронные носители персональных данных (диски, флеш-карты) в шкафы;
 - отключить технические средства и электроприборы от сети, выключить освещение;
 - закрыть окна; закрыть двери.
8. Перед открытием помещений, в которых ведется обработка персональных данных, работники, имеющие право доступа в помещения, обязаны провести внешний осмотр с целью установления целостности двери и замка;
9. При обнаружении неисправности двери и запирающих устройств работники обязаны:
 - не вскрывая помещение, в котором ведется обработка персональных данных, доложить заведующему РОО;
 - в присутствии не менее двух иных работников, включая заведующего РОО, вскрыть помещение и осмотреть его;
 - составить акт о выявленных нарушениях и передать его заведующему РОО для организации служебного расследования.
10. Право самостоятельного входа в помещения, где обрабатываются персональные данные, имеют только работники, непосредственно работающие в данном помещении.

Иные работники имеют право пребывать в помещениях, где обрабатываются персональные данные, только в присутствии работников, непосредственно работающих в данных помещениях.

11. При работе с информацией, содержащей персональные данные, двери помещений должны быть всегда закрыты.

Присутствие иных лиц, не имеющих права доступа к персональным данным, должно быть исключено.

12. Техническое обслуживание компьютерной и организационной техники, сопровождение программных средств, уборка помещения, в котором ведется обработка персональных данных, а также проведение других работ осуществляются в присутствии работника, работающего в данном помещении.

13. В случае необходимости принятия в нерабочее время экстренных мер при срабатывании пожарной или охранной сигнализации, авариях в системах энерго-, водо- и теплоснабжения помещение, в котором ведется обработка персональных данных, вскрывается комиссией в составе не менее двух человек.

14. Ответственность за соблюдение порядка доступа в помещения, в которых ведется обработка персональных данных, возлагается на работников, обрабатывающих персональные данные.

Приложение

Перечень

мест хранения персональных данных (ПДн), обрабатываемых в районном отделе образования администрации Павинского муниципального района

№ п/п	Подразделения	Место назначения	Наименование документа, содержащего ПДн
1	Районный отдел образования	Помещение районного отдела образования	Приказы по основной деятельности Приказы по личной составу Трудовые книжки Личные дела Списки руководителей образовательных учреждений. Списки педагогических кадров образовательных учреждений Протоколы заседаний аттестационных комиссий. Списки детей, проживающих на территории Павинского муниципального района. Заявления о предоставлении мест детям в учреждениях, реализующую программу дошкольного образования. Списки выпускников 9 и 11 классов. Заявления кандидатов в качестве общественного наблюдателя при проведении ГИА. Результаты ГИА. Копии протоколов муниципального этапа всероссийской олимпиады школьников. Информация о семьях с детьми получающих МСП

**Уведомление об уничтожении,
(изменении, прекращении обработки, устранении нарушений
персональных данных)**

Уважаемый _____.
(фамилия, имя, отчество)

В связи с _____

(недостоверностью, выявлением неправомерных действий с Вашими персональными данными, достижением цели обработки, отзывом

Вами согласия на обработку, другие причины)

сообщаем Вам, что обработка Ваших персональных данных

_____.
(перечислить)

прекращена и указанная информация подлежит уничтожению (изменению).

дата

подпись

расшифровка подписи

Настоящее уведомление на руки получил:

дата

подпись

расшифровка