

Министерство образования и науки Российской Федерации
государственное бюджетное общеобразовательное учреждение Самарской области
средняя общеобразовательная школа № 2
«Образовательный центр» с.Кинель-Черкассы
муниципального района Кинель-Черкасский Самарской области
(ГБОУ СОШ № 2 «ОЦ» с.Кинель-Черкассы)

П Р И К А З

15 января 2016 г.

№ 01-3/4-02

Об утверждении Положения об обработке и защите персональных данных

В соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее - Закон № 152-ФЗ), Федеральным законом от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации», п р и к а з ы в а ю:

1. Утвердить Положение об обработке и защите персональных данных (далее - Положение) государственного бюджетного общеобразовательного учреждения средней общеобразовательной школы №2 «Образовательный центр» с.Кинель-Черкассы муниципального района Кинель-Черкасский Самарской области, в соответствии с приложением №1 к настоящему приказу.
2. Разместить настоящий приказ на официальном сайте учреждения в течение десяти рабочих дней со дня издания настоящего приказа.
3. Считать утратившим силу положение об обработке и защите персональных данных, утвержденное приказом ГБОУ СОШ №2 «ОЦ» с.Кинель-Черкассы от 30.01.2012 г. № 13/1-од «Об утверждении локальных актов».
4. Контроль исполнения настоящего приказа возложить на заместителя директора по ИОС Постникову С.Г.

Директор



О.Е.Иванова

Утверждено приказом
ГБОУ СОШ №2 «ОЦ» с.Кинель-Черкассы
от 15.01.2016 № 01-3/4-од

ПОЛОЖЕНИЕ
об обработке и защите персональных данных
государственного бюджетного общеобразовательного учреждения
средней общеобразовательной школы №2 «Образовательный центр»
с.Кинель-Черкассы муниципального района Кинель-Черкасский Самарской области

1. Общие положения

- 1.1. Настоящее Положение об обработке и защите персональных данных (далее - Положение) государственного бюджетного общеобразовательного учреждения средней общеобразовательной школы №2 «Образовательный центр» с.Кинель-Черкассы муниципального района Кинель-Черкасский Самарской области (далее – Учреждение) разработано на основании Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных" (далее - Закон № 152-ФЗ), Федерального закона от 29.12.2012 № 273 ФЗ "Об образовании в Российской Федерации", Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановления Правительства РФ от 15.09.2008 № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", в соответствии с Трудовым кодексом Российской Федерации, Конституцией Российской Федерации, Гражданским кодексом Российской Федерации, иными нормативными актами, действующими на территории Российской Федерации, а также Уставом и иными локальными актами Учреждения.
- 1.2. Цель разработки Положения - определение порядка обработки персональных данных работников Учреждения, обучающихся (воспитанников) и их родителей (законных представителей) и иных субъектов персональных данных, персональные данные которых подлежат обработке, на основании полномочий Учреждения, как оператора персональных данных; обеспечение защиты прав и свобод человека и гражданина, в т.ч. работников Учреждения, учащихся (воспитанников) и их родителей (законных представителей), при обработке их персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.
- 1.3. Порядок ввода в действие и изменения Положения.
 - 1.3.1. Настоящее Положение вступает в силу с момента его утверждения руководителем Учреждения и действует бессрочно, до замены его новым Положением.
 - 1.3.2. Все изменения в Положение вносятся приказом руководителя.
- 1.4. Все работники Учреждения должны быть ознакомлены с настоящим Положением под роспись.
- 1.5. Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении 75 лет срока их хранения, или продлевается на основании заключения экспертной комиссии Учреждения, если иное не определено законом.

II. Основные понятия и состав персональных данных

2.1. Для целей настоящего Положения используются следующие основные понятия:

- персональные данные - любая информация, относящаяся к определённому или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, позволяющая идентифицировать его личность.
- обработка персональных данных - сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение персональных данных;
- конфиденциальность персональных данных - обязательное для соблюдения назначенного ответственного лица, получившего доступ к персональным данным субъектов, требование не допускать их распространения без согласия субъекта или иного законного основания;
- распространение персональных данных - действия, направленные на передачу персональных данных субъектов определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных субъектов в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным субъектов каким-либо иным способом;
- использование персональных данных - действия (операции) с персональными данными, совершаемые должностным лицом Учреждения в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъектов либо иным образом затрагивающих их права и свободы или права и свободы других лиц;
- блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;
- уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;
- обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту;
- общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.
- информация - сведения (сообщения, данные) независимо от формы их представления.
- документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.
- субъект персональных данных – Работники, состоящие в трудовых отношениях с Учреждением, обучающиеся (воспитанники) Учреждения и их родители (законные представители).

2.2. Комплекс документов, сопровождающий процесс оформления трудовых отношений с работником в Учреждении при его приеме, переводе и увольнении.

2.2.1. Информация, представляемая работником при поступлении на работу в Учреждение, должна иметь документальную форму. При заключении трудового договора в соответствии со ст. 65 Трудового кодекса Российской Федерации лицо, поступающее на работу, предъявляет работодателю:

- паспорт или иной документ, удостоверяющий личность;
- трудовая книжка, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства, либо трудовая книжка у работника отсутствует в связи с ее утратой или по другим причинам;
- страховое свидетельство государственного пенсионного страхования;
- документы воинского учета - для военнообязанных и лиц, подлежащих воинскому учету;
- документ об образовании, о квалификации или наличии специальных знаний, при поступлении на работу, требующую специальных знаний или специальной подготовки;
- справка об отсутствии или наличии судимости;

2.2.2. В процессе трудовых отношений с работниками в Учреждении создаются и хранятся следующие группы документов, содержащие данные о работниках в единичном или сводном виде:

2.2.2.1. Документы, содержащие персональные данные работников - комплексы документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении; комплекс материалов по анкетированию, тестированию; проведению собеседований с кандидатом на должность; подлинники и копии приказов по личному составу; личные дела и трудовые книжки работников; дела, содержащие основания к приказу по личному составу; дела, содержащие материалы аттестации работников; служебных расследований; справочно-информационный банк данных по персоналу (картотеки, журналы); подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству Учреждения, руководителям структурных подразделений; копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения.

2.2.2.2. Документация по организации работы Учреждения (должностные инструкции работников, приказы, распоряжения, указания руководства Учреждения); документы по планированию, учету, анализу и отчетности в части работы с персоналом Учреждения.

2.3. Комплекс документов, сопровождающий процесс работы с обучающимися (воспитанниками).

2.3.1. Информация, представляемая родителями (законными представителями) в образовательное учреждение, должна иметь документальную форму. Родители обучающихся (воспитанников), либо их представители предъявляют следующие документы:

- документы, удостоверяющие личность обучающегося (воспитанника) (свидетельство о рождении или паспорт);
- документы о месте проживания;
- документы о составе семьи;
- паспорт или иной документ, удостоверяющий личность родителей (законных представителей) обучающегося (воспитанника);
- документы о получении образования, необходимого для поступления в соответствующий класс (личное дело, справка с предыдущего места учебы и т.п.);

- документы о состоянии здоровья (сведения об инвалидности, о наличии хронических заболеваний, медицинское заключение об отсутствии противопоказаний для обучения в образовательном учреждении конкретного вида и типа, о возможности изучения предметов, представляющих повышенную опасность для здоровья и т.п.);
 - документы, подтверждающие права на дополнительные гарантии и компенсации по определенным основаниям, предусмотренным законодательством (родители-инвалиды, неполная семья, ребенок-сирота и т.п.);
- 2.3.2. В процессе образовательных отношений с обучающимися (воспитанниками) в Учреждении создаются и хранятся следующие группы документов, содержащие данные об обучающихся (воспитанниках) в единичном или сводном виде:
- 2.3.2.1. Документы, содержащие персональные данные обучающихся (воспитанников) - комплексы документов, сопровождающие процесс зачисления, отчисления, перевода в другой класс, другое образовательное учреждение; комплекс материалов по анкетированию, тестированию; проведению аттестации; подлинники и копии приказов по личному составу; личные дела; дела, содержащие основания к приказу по личному составу; дела, содержащие материалы аттестации; служебных расследований; справочно-информационный банк данных (картотеки, журналы); подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству Учреждения, руководителям структурных подразделений; копии отчетов, направляемых в государственные органы статистики, вышестоящие органы управления и другие учреждения.
- 2.4. Вне каких-либо информационных систем персональных данных Учреждение обрабатывает персональные данные иных лиц, полученные любым законным путем при заключении и исполнении договоров, либо исполнении ненормативных правовых актов и иной не запрещенной законом деятельности.
- 2.5. Состав персональных данных работников, обучающихся (воспитанников) и их родителей (законных представителей) определен в «Перечне сведений, составляющих персональные данные» (Приложение 1).

III. Порядок получения персональных данных

- 3.1. Персональные данные следует получать непосредственно у субъекта, либо у законного представителя.
- 3.2. Перед началом обработки персональных данных необходимо получить у субъекта или его законного представителя согласие на обработку персональных данных в письменной форме, в соответствии с утвержденной формой такого Согласия (Приложение 6).
- 3.2.1. Письменное согласие субъекта на обработку своих персональных данных должно включать в себя:
- 1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
 - 2) наименование и адрес оператора (Учреждения), получающего согласие субъекта персональных данных;
 - 3) цель обработки персональных данных;
 - 4) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
 - 5) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых способов обработки персональных данных;

б) срок, в течение которого действует согласие, а также порядок его отзыва;

7) подпись субъекта персональных данных.

3.2.2. Согласия не требуется в следующих случаях:

- персональные данные являются общедоступными;
- обработка персональных данных субъекта необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия работника или родителя невозможно;
- обработка персональных данных необходима для установления или осуществления прав их субъекта или третьих лиц либо в связи с осуществлением правосудия;
- обработка персональных данных осуществляется в соответствии с законодательством РФ об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, об исполнительном производстве, с уголовно-исполнительным законодательством РФ;
- обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством;
- по требованию полномочных государственных органов в случаях, предусмотренных федеральным законом;
- в случаях если обработка персональных данных работников осуществляется на основании Трудового кодекса РФ или иного Федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия работодателя;
- обработка персональных данных осуществляется в целях исполнения трудового договора; договора о предоставлении образования;
- обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных.

3.2.3. Субъект персональных данных принимает решение о предоставлении своих персональных данных и дает письменное согласие на их обработку своей волей и в своих интересах. Он может в любой момент и без объяснения причин отозвать согласие на обработку своих персональных данных, совершение отдельных операций с ними либо использование в отдельных целях.

3.2.4. В случае отзыва субъектом своего согласия на обработку персональных данных, Учреждение, в течение трёх рабочих дней прекращает обработку его персональных данных и уничтожает их в срок до 90 рабочих дней (кроме персональных данных, подлежащих архивному хранению на основании норм федерального законодательства), о чем уведомляет субъекта любым доступным способом.

3.2.5. В случае недееспособности субъекта персональных данных или в результате его смерти согласие на обработку его персональных данных или отзыв персональных данных субъекта дает в письменной форме законный представитель субъекта персональных данных или его законный наследник.

3.3. Учреждение не вправе:

- требовать от субъекта предоставления информации о его национальности и расовой принадлежности, политических и религиозных убеждениях и частной жизни.
- получать и обрабатывать персональные данные субъекта о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных Федеральным законом.

- 3.4. Если персональные данные субъекта можно получить исключительно у третьей стороны, то субъект должен быть уведомлен об этом заранее и от него необходимо получить письменное согласие (Приложение 4). Учреждение должно сообщить субъекту о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа субъекта представить письменное согласие на их получение.
- 3.5. В случае увольнения (отчисления) субъекта оператор обязан незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий тридцати рабочих дней с даты достижения цели обработки персональных данных, если иное не предусмотрено законодательством РФ либо договором с субъектом.

IV. Порядок обработки, передачи и хранения персональных данных

4.1. Особенности обработки персональных данных

- 4.1.1. Учреждение определяет объем, содержание обрабатываемых персональных данных субъектов персональных данных (работников, обучающихся (воспитанников) и их родителей (законных представителей)), руководствуясь Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом Российской Федерации от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации», настоящим Положением, локальными актами ОУ.
- 4.1.2. Обработка персональных данных работников осуществляется исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, а также обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.
- 4.1.3. Обработка персональных данных обучающихся (воспитанников) и их родителей (законных представителей) может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, регламентирующих образовательную деятельность Учреждения; содействия обучающимся в обучении, проведении государственной итоговой аттестации, при поступлении в ВУЗы, колледжи и иные образовательные организации, трудоустройстве; обеспечения их личной безопасности; контроля качества обучения и обеспечения сохранности имущества,
- 4.1.4. Должностные лица Учреждения, в обязанности которых входит обработка персональных данных субъектов, обеспечивают каждому субъекту возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.
- 4.1.5. При принятии решений, затрагивающих интересы субъекта, Учреждение не имеет права основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или электронного получения.
- 4.1.6. Обработка персональных данных субъектов может осуществляться как с использованием средств автоматизации, так и без использования таковых.
- 4.1.7. Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

4.1.8. Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее.

4.2. Обработка персональных данных, осуществляемая без использования средств автоматизации

4.2.1. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, обособляются от иной информации, путем фиксации их на отдельных материальных носителях персональных данных (далее - материальные носители).

4.2.2. 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.

4.2.3. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется оператором 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 Школы.

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

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес оператора, 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 оператором способов обработки персональных данных;
- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своей согласии на обработку персональных данных, осуществляемую без использования средств автоматизации,- при необходимости получения письменного согласия на обработку персональных данных;
- 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;
- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

4.2.5. При ведении журналов (классные журналы, журналы регистрации, журналы посещений и др.), содержащих персональные данные субъектов, следует учитывать, что необходимость их ведения предусмотрена федеральными законами и локальными актами Учреждения, содержащими сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации,

способах фиксации и составе информации, запрашиваемой у субъектов персональных данных, перечне лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журналов, сроках обработки персональных данных, а также, что копирование содержащейся в них информации не допускается.

4.2.6. 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, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

- при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;
- при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

4.2.7. 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, вымарывание).

4.2.8. 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.

4.3. Передача и хранение персональных данных

4.3.1. При передаче персональных данных работников, обучающихся (воспитанников) и их родителей (законных представителей) должны соблюдаться следующие требования:

4.3.1.1. Не сообщать персональные субъектов третьей стороне без письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью, а также в случаях, установленных федеральным законом.

4.3.1.2. Не сообщать персональные данные субъектов в коммерческих целях без его письменного согласия.

4.3.1.3. Предупредить лиц, получивших персональные субъектов, 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. Лица, получившие персональные данные субъекта, обязаны соблюдать конфиденциальность. Данное положение не распространяется на обмен персональными данными субъектов в порядке, установленном федеральными законами;

- 4.3.1.4. Осуществлять передачу персональных данных субъектов в пределах Учреждения в соответствии с настоящим Положением.
- 4.3.1.5. Передавать персональные данные работника представителям работников в порядке, установленном Трудовым кодексом Российской Федерации, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функции.
- 4.3.1.6. Передача информации, содержащей сведения о персональных данных субъектов, по телефону, факсу, электронной почте без письменного согласия субъекта запрещается.
- 4.3.2. Хранение персональных данных.
 - 4.3.2.1. Личные дела и документы, содержащие персональные данные субъектов, хранятся в приемной Учреждения в запирающихся шкафах (сейфах), обеспечивающих защиту от несанкционированного доступа.
 - 4.3.2.2. Персональные данные могут храниться также в электронном виде и в автоматизированных информационных системах.
 - 4.3.2.3. Права доступа к персональным данным в автоматизированных системах разграничены между различными категориями пользователей. Вход в систему осуществляется только при введении личного пароля пользователя.
 - 4.3.2.4. Помещения, в котором хранятся персональные данные субъектов, должны быть оборудованы надежными замками.
 - 4.3.2.5. Персональные компьютеры, в которых содержатся персональные данные, должны быть защищены паролями доступа.
 - 4.3.2.6. Места хранения персональных данных и ответственные за обеспечение сохранности материальных носителей персональных данных определены в «Перечне мест хранения персональных данных и ответственных лиц» (Приложение 3)

V. Доступ к персональным данным

- 5.1. Персональные данные защищаются от несанкционированного доступа в соответствии с нормативными правовыми актами РФ, нормативно-распорядительными актами и рекомендациями регулирующих органов в области защиты информации, а также утвержденными регламентами и инструкциями Учреждения.
- 5.2. Доступ к персональным данным субъектов персональных данных разрешен только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы им для выполнения конкретных функций.
- 5.3. Внутренний доступ (доступ внутри Учреждения) определяется перечнем должностных лиц, имеющих доступ к персональным данным субъектов.
 - 5.3.1. Допуск к персональным данным субъекта могут иметь только те работники Учреждения, которым персональные данные необходимы в связи с исполнением ими своих трудовых обязанностей.
 - 5.3.2. Процедура оформления допуска к персональным данным представляет собой следующую строгую последовательность действий:
 - ознакомление работника с настоящим Положением, «Инструкцией о порядке работы с персональными данными» и другими локальными нормативно-правовыми актами Учреждения, касающимися обработки персональных данных;
 - истребование с работника «Обязательства о неразглашении конфиденциальной информации» (Приложение 5);

- 5.3.3. Каждый работник должен иметь доступ к минимально необходимому набору персональных данных субъектов, необходимых ему для выполнения служебных (трудовых) обязанностей.
- 5.3.4. Работникам, не имеющим надлежащим образом оформленного допуска, доступ к персональным данным субъектов запрещается.
- 5.3.5. Работники Учреждения не имеют права обрабатывать персональные данные, доступ к которым они получили в связи с исполнением трудовых обязанностей, в личных или иных, отличных от установленных Учреждением целей.
- 5.3.6. Порядок разграничения прав доступа к персональным данным определен в Приложении № 4
- 5.4. К числу массовых потребителей персональных данных вне Учреждения (внешний доступ) можно отнести государственные и негосударственные функциональные структуры:
- налоговые инспекции;
 - правоохранительные органы;
 - органы статистики;
 - страховые агентства;
 - военкоматы;
 - органы социального страхования;
 - пенсионные фонды;
 - подразделения муниципальных органов управления.
- 5.4.1. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.
- 5.4.2. Ответы на письменные запросы других организаций и учреждений в пределах их компетенции и предоставленных полномочий даются в письменной форме на бланке предприятия и в том объеме, который позволяет не разглашать излишний объем персональных сведений субъектов.
- 5.4.3. Персональные данные работника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого работника.
- 5.4.4. В случае развода бывшая супруга (супруг) имеют право обратиться в организацию с письменным запросом о размере заработной платы работника без его согласия. (УК РФ).

VI. Организация защиты персональных данных

6.1. Обеспечение конфиденциальности и безопасности персональных данных

- 6.1.1. Учреждение обеспечивает конфиденциальность всех обрабатываемых им персональных данных, за исключением общедоступных. Режим конфиденциальности не установлен относительно общедоступных персональных данных, которые приобрели такой статус волей субъекта персональных данных и при изменении обстоятельств могут вновь приобрести статус конфиденциальных по желанию субъекта.
- 6.1.2. Учреждение при обработке персональных данных принимает необходимые организационные, инженерно-технические, программно-аппаратные меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.
- 6.1.3. Конфиденциальность и безопасность персональных данных обеспечиваются путём применения физических, экономических, организационных, правовых, программно-аппаратных и инженерно-технических мер защиты информации. Для защиты информации, обрабатываемой в автоматизированных ИСПДн, используются инженерно-технические, программные и программно-аппаратные

средства защиты в соответствии с требованиями законодательства, которые устанавливаются федеральным органом исполнительной власти, исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации в пределах их полномочий.

6.1.4. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных субъектов.

6.1.5. По возможности персональные данные обезличиваются.

6.2. Защита персональных данных

6.2.1. Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

6.2.2. Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

6.2.3. Защита персональных данных представляет собой жестко регламентированный и динамически технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности Учреждения.

6.2.4. Защита персональных данных субъектов от неправомерного их использования или утраты должна быть обеспечена Учреждением за счет его средств, и в порядке, установленном федеральным законом.

6.2.5. «Внутренняя защита».

6.2.5.1. Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителями и работниками Учреждения.

6.2.5.2. Для обеспечения внутренней защиты персональных данных субъектов необходимо соблюдать ряд мер:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между работниками;
- рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание работником требований нормативно – методических документов по защите информации и сохранении тайны;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором хранятся персональные данные;
- организация порядка уничтожения информации;
- организация процедуры резервирования данных для последующего восстановления работоспособности информационных систем при полной или

частичной потере информации, вызванной сбоями или отказами аппаратного или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.);

- проведение внутреннего контроля соответствия требованиям обработки персональных данных;
- своевременное выявление нарушения требований разрешительной системы доступа работниками Учреждения;
- воспитательная и разъяснительная работа с работниками Учреждения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- разработка комплекса мер по организации защиты персональных данных.

6.2.5.3. Не допускается выдача личных дел. Личные дела работников могут выдаваться на рабочие места только директору, делопроизводителю и в исключительных случаях - руководителю структурного подразделения (например, при подготовке материалов для аттестации работника). Личные дела обучающихся – только директору, делопроизводителю и классному руководителю.

6.2.6. «Внешняя защита».

6.2.6.1. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

6.2.6.2. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности Учреждения, посетители, работники других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов.

6.2.6.3. Для обеспечения внешней защиты персональных данных необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;
- пропускной режим Учреждения;
- технические средства охраны, сигнализации;
- порядок охраны территории, зданий, помещений, транспортных средств;
- требования к защите информации при интервьюировании и собеседованиях.

6.2.9. Кроме мер защиты персональных данных, установленных законодательством, Учреждение, работники и законные представители обучающихся (воспитанников) могут вырабатывать совместные меры защиты персональных данных.

6.3. Особенности обеспечения безопасности персональных данных при их обработке в информационной системе персональных данных

6.3.1. Состав информационных систем персональных данных Учреждения и их характеристика определяется «Перечнем информационных систем персональных данных» (Приложение 2).

6.3.2. 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.

- 6.3.3. 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.
- 6.3.4. Средства защиты информации, применяемые в информационных системах, в обязательном порядке проходят процедуру оценки соответствия в установленном законодательством РФ порядке.
- 6.3.5. 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.
- 6.3.6. 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.
- 6.3.7. Безопасность персональных данных при их обработке в информационной системе персональных данных обеспечивает специалист, ответственный за организацию обработки персональных данных в ИСПДн (администратор безопасности ИСПДн).
- 6.3.8. При обработке персональных данных в информационной системе должно быть обеспечено:
- проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
 - своевременное обнаружение фактов несанкционированного доступа к персональным данным;
 - недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
 - возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
 - постоянный контроль над обеспечением уровня защищенности персональных данных.
- 6.3.9. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают:
- определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;
 - разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;
 - проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;
 - установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;
 - обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
 - учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

- учет лиц, допущенных к работе с персональными данными в информационной системе;
 - контроль по соблюдению условий использования средств защиты информации, предусмотренных эксплуатационной и технической документации;
 - 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;
 - описание системы защиты персональных данных. Осуществление мероприятий по обеспечению безопасности персональных данных при их обработке в информационной системе уполномоченным лицом возлагается на ответственного за организацию обработки персональных данных.
- 6.3.10. При обнаружении нарушений порядка предоставления персональных данных уполномоченное лицо незамедлительно приостанавливает предоставление персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин.
- 6.3.11. Иные требования по обеспечению безопасности информации и средств защиты информации в Учреждении выполняются в соответствии с требованиями федеральных органов исполнительной власти и органов исполнительной власти Самарской области.

VII. Права субъектов персональных данных

- 7.1. На основании требований ст. 89 ТК РФ и ст. 14 152-ФЗ, в целях обеспечения защиты персональных данных, хранящихся в Учреждении, субъекты персональных данных имеют право:
- на полную информацию о факте обработки, перечне и содержании персональных данных, находящихся в распоряжении Учреждения, а также о цели их обработки, о правовых основаниях обработки, о способах обработки этих данных, применяемых Учреждением, об источнике их получения и о лицах (кроме работников Учреждения), получивших доступ к персональным данным субъекта;
 - свободный бесплатный доступ к своим персональным данным по его персональному запросу или запросу его законного представителя, включая право на получение копии любой записи, содержащей персональные данные субъекта, за исключением случаев, предусмотренных федеральным законом;
 - определение своих представителей для защиты своих персональных данных;
 - получение информации о сроках обработки персональных данных, в том числе о сроках их хранения, возможного блокирования и уничтожения;
 - получение сведений о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
 - доступ к относящимся к субъекту медицинским данным с помощью медицинского специалиста по его выбору;
 - требовать об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований федерального законодательства.
 - требовать об извещении Учреждением всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта, обо всех произведённых в них исключениях, исправлениях или дополнениях;

- получение сведений о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных;
 - требовать, в соответствии с ч. 5 ст. 14 152-ФЗ, о блокировании или уничтожении своих персональных данных (если эти требования не противоречат федеральному законодательству РФ);
 - принятие предусмотренных Федеральным законодательством мер по защите своих прав, в том числе, обжалование в суд любых неправомерных действий или бездействий Учреждения при обработке и защите его персональных данных.
- 7.2. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено на основании федеральных законов, в том числе, на основании требований ч. 8 ст. 14 152-ФЗ.
- 7.3. В случае если лицо, обратившееся с запросом, не обладает соответствующими полномочиями на получение персональных данных, либо отсутствует письменное согласие субъекта на передачу его персональных данных, Учреждение вправе отказать в предоставлении персональных данных. В этом случае лицу, обратившемуся с запросом, направляется письменный мотивированный отказ в предоставлении запрашиваемой информации.
- Порядок рассмотрения запросов субъектов утверждается отдельными правилами, регламентами.
- 7.4. Во всех случаях отказ субъекта от своих прав на сохранение и защиту тайны недействителен.

VIII. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

- 8.1. Персональная ответственность – одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.
- 8.2. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.
- 8.3. Каждый работник организации, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.
- 8.4. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) влечет дисциплинарную, административную, гражданско–правовую или уголовную ответственность граждан и юридических лиц.