

Принято
педагогическим советом
МБОУ СОШ №51 г. Пензы.

Протокол № 9
от 30 августа 2016 г.

Утверждаю
Директор
МБОУ СОШ № 51 г. Пензы

(О.Д. Кулинская)
Приказ № 140/1-оп от
01.09.2016 г.

***Положение
об обработке и защите
персональных данных
в МБОУ СОШ №51 г. Пензы***

1. Термины и определения

В настоящем Положении об обработке и защите персональных данных в МОУ СОШ № 51 г. Пензы используются основные понятия и термины, определённые Федеральными законами от 27.07.2006 № 152-ФЗ «О персональных данных» (с последующими изменениями) и № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с последующими изменениями).

1) **персональные данные** - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных);

2) **обработка персональных данных** - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;

- распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

- использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или 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 персональных данных;

3) **информационная система персональных данных (ИСПДн)**- информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

4) **конфиденциальность персональных данных** - обязательное для соблюдения всем лицам, получившим доступ к персональным данным, требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;

5) **общедоступные персональные данные** - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

2. Общие положения

2.1. Целью Положения об обработке и защите персональных данных в МОУ СОШ № 51 г. Пензы (далее – Учреждение) является обеспечение защиты персональных данных от несанкционированного доступа, неправомерного их использования или утраты.

2.2. Настоящее Положение устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных структурных подразделений Учреждения.

2.3. Настоящее Положение разработано в соответствии с:

- Конституцией Российской Федерации;
- Трудовым кодексом Российской Федерации;
- Кодексом об административных правонарушениях Российской Федерации;
- Гражданским кодексом Российской Федерации;
- Уголовным кодексом Российской Федерации;
- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (с последующими изменениями);
- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с последующими изменениями);
- Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановлением Правительства Российской Федерации от 17.11.2007 № 781 г. Москва «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в ИСПДн»;
- Приказ ФСТЭК от 13.02.2008 г. № 55/86/20 «Об утверждении порядка проведения классификации ИСПДн».

2.4. Обработка персональных данных в Учреждении должна осуществляться на основе принципов, определенных в статье 5 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (с последующими изменениями).

2.5. Ответственные по разработке и выполнению мероприятий по обеспечению безопасности персональных данных при их обработке в Учреждении, а также координации работ по защите конфиденциальной информации назначаются приказом.

2.6. Лица, производящие обработку персональных данных или имеющие к ним доступ, являются ответственными за защиту персональных данных.

2.7. Обработка персональных данных, содержащихся в информационных системах персональных данных либо извлеченных из таких систем МОУ СОШ № 51, осуществляется с использованием средств автоматизации и без них, т.е. является смешанной (автоматизированной и неавтоматизированной).

2.8. В части работы с обращениями граждан, порядок обработки и защиты персональных данных организуется в соответствии с Федеральным законом от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» (с последующими изменениями) и данным Положением.

2.9. Настоящее Положение является обязательным для исполнения всеми работниками Учреждения, имеющими доступ к персональным данным.

3. Порядок определения защищаемой информации

3.1. В Учреждении на основании утвержденного Указом Президента Российской Федерации от 06.03.1997 № 188 (с последующими изменениями) Перечня сведений конфиденциального характера, в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с последующими изменениями), определяется и утверждается сводный перечень персональных данных, обрабатываемых в МБОУ СОШ № 51 г. Пензы, в том числе в ИСПДн.

4. Условия сбора и обработки персональных данных

4.1. Сбор персональных данных может осуществляться как путем представления их самим субъектом, так и путем получения из иных источников. Если персональные данные субъекта возможно получить только у третьей стороны, то субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Сотрудники, допущенные к обработке персональных данных должны сообщить (в том числе устно) субъекту о целях, предполагаемых источниках и способах получения персональных данных, а так же о характере подлежащих получению персональных данных и последствиях отказа субъекта дать письменное согласие на их получение.

4.2. Обработка персональных данных в Учреждении осуществляется только после получения согласия от субъекта персональных данных, составленного по форме согласно приложению № 1 к настоящему Положению или в случаях, предусмотренных частью 2 статьи 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (с последующими изменениями). В случаях, непосредственно связанных с вопросами трудовых отношений, данные о частной жизни субъекта (информация о жизнедеятельности в сфере семейных, бытовых, личных отношений) могут быть получены и обработаны сотрудниками, допущенными к обработке персональных данных, только с его письменного согласия.

4.3. Учреждение не имеет права получать и обрабатывать персональные данные субъекта о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.

4.4. Все меры конфиденциальности при сборе, обработке и хранении персональных данных субъекта распространяются как на бумажные, так и на электронные носители информации.

4.5. В соответствии с должностными инструкциями работников школы определяется и утверждается список пользователей ИСПДн МБОУ СОШ № 51. Сотрудники, допущенные к обработке персональных данных, в обязательном порядке под роспись знакомятся с настоящим Положением и инструкцией пользователя ИСПДн МБОУ СОШ № 51, подписывают обязательство о неразглашении информации, содержащей персональные данные.

5. Хранение и использование персональных данных

5.1. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

5.2. Хранение персональных данных должно происходить в порядке, исключающем их утрату или их неправомерное использование.

5.3. В Учреждении ежегодно определяется список лиц, допущенных к обработке ПДн, и разрешительная система доступа. Право доступа к персональным данным субъекта в Учреждении имеют:

- Руководитель Учреждения;
- Заместители Руководителя Учреждения;
- сам субъект персональных данных;
- работники Учреждения, допущенные к работе с персональными данными, при выполнении ими своих служебных обязанностей.

5.4. Приказом директора определяются места хранения материальных носителей, содержащих ПДн с описанием требований к защите от несанкционированного доступа и персональный список ответственных за хранение и защиту материальных носителей ПДн.

6. Передача персональных данных субъектов

6.1. Передача персональных данных субъекта возможна только с согласия субъекта или в случаях, предусмотренных законодательством.

6.2. При передаче персональных данных субъекта уполномоченные Учреждением сотрудники должны соблюдать следующие требования:

- не сообщать персональные данные субъекта третьей стороне без письменного согласия субъекта, за исключением случаев, установленных федеральным законом;

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

- не запрашивать информацию о состоянии здоровья субъекта персональных данных, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовых функций;

- предупредить лиц, получающих персональные данные субъекта, 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, получающие персональные данные субъекта, обязаны соблюдать режим защиты персональных данных;

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

6.3. Передача персональных данных от Учреждения или его представителей внешнему оператору допускается в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

6.4. При поступлении в школу законные представители учащихся и работники заполняют согласия на обработку ПДн, в том числе передачу третьим лицам.

7. Права субъектов по обеспечению защиты персональных данных, хранящихся в Учреждении

7.1. В целях защиты персональных данных, хранящихся в Учреждении, субъект имеет право:

- на полную информацию о своих персональных данных и обработке этих данных;
- требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением требований Трудового кодекса Российской Федерации или иного федерального закона;

- определять своих представителей для защиты своих персональных данных;

- на сохранение и защиту своей личной и семейной тайны;

- на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные, за исключением случаев, предусмотренных федеральным законодательством;

- на обжалование в суде любых неправомерных действий работодателя при обработке и защите его персональных данных.

8. Требования к обработке и защите персональных данных в информационных системах Учреждения

8.1. Обработка персональных данных в Учреждении организуется на основании постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

8.2. Защита персональных данных должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных были выполнены следующие требования:

- определены места хранения персональных данных (материальных носителей),
- обеспечено раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях;
- соблюдены условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

8.3. Применяемые меры по защите персональных данных в ИСПДн Учреждения должны быть направлены на:

- ограничение доступа персонала и посторонних лиц в помещения, где размещены информационные системы персональных данных и хранятся материальные носители персональных данных;
- организацию учёта и надёжного хранения материальных носителей персональных данных, их обращения, исключающее хищение, подмену и уничтожение;
- размещение дисплеев и других средств отображения информации, исключающее её несанкционированный просмотр.

8.4. Обработка персональных данных на базе автономных ПЭВМ в Учреждении ведется с использованием лицензионного программного обеспечения, в том числе антивирусной защиты.

8.5. Порядок защиты персональных данных на базе автономных ПЭВМ в Учреждении определен п. 5.5 «Специальных требований и рекомендаций по технической защите конфиденциальной информации», утвержденных приказом Гостехкомиссии России от 30.08.2002 № 282 (с последующими изменениями).

9. Порядок привлечения специализированных сторонних организаций к разработке информационных систем персональных данных и средств защиты информации в Учреждении

9.1. Порядок привлечения специализированных сторонних организаций к разработке и эксплуатации новых информационных систем персональных данных, их задачи и функции на различных стадиях создания и эксплуатации определяются руководителями структурных подразделений Учреждения, у которых находится информационная система, исходя из особенностей информационных систем и по согласованию с ответственным сотрудником Учредителя.

9.2. Для выбора и реализации методов и способов защиты информации в информационной системе Учреждения может привлекаться организация, имеющая оформленную в установленном порядке лицензию на осуществление деятельности по технической защите конфиденциальной информации.

10. Ответственность за нарушение норм, регулирующих получение, обработку и защиту персональных данных

10.1. Персональная ответственность – одно из главных требований к организации функционирования в Учреждении системы защиты персональных данных и обязательное условие обеспечения эффективности этой системы.

10.2. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено в соответствии с законодательством.

10.3. Ответственные работники Учреждения, виновные в нарушении норм и требований действующего законодательства, регулирующих обработку и защиту персональных данных, несут ответственность в соответствии с действующим законодательством.

11. Уничтожение персональных данных

11.1. 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.

11.2. Уничтожение носителей персональных данных осуществляется в течение 30 дней с момента письменного отзыва субъекта согласия на обработку персональных данных или истечения сроков обработки и хранения персональных данных.

11.3. Для проведения процедуры уничтожения материальных носителей персональных данных приказом директора создается комиссия, состоящая из трех работников МБОУ СОШ № 51 г. Пензы, имеющих право на обработку персональных данных.

11.4. Бумажные носители персональных данных (документы, их копии, выписки), уничтожаются путём измельчения на мелкие части, исключающие возможность последующего восстановления информации или сжигаются.

11.4. Машиночитаемые носители (компакт-диски CD-R/RW или DVD-R/RW, дискеты 3,5, флеш-носители) по истечению сроков обработки и хранения на них персональных данных, подлежат уничтожению путем деформирования, нарушения единой целостности носителя или его сжигания.

11.4. Уничтожение носителей персональных данных в электронном и магнито-электронном виде (файлы, папки, электронные архивы на жестком диске), расположенные на жестком диске информационной системы персональных данных, удаляются средствами операционной системы компьютера с последующим «очищением корзины».

11.5. В ходе процедуры уничтожения носителей или форматирования носителя необходимо присутствие всех членов комиссии. По окончании уничтожения бумажных носителей комиссией составляется Акт об уничтожении бумажных носителей персональных данных и направляется на утверждение директору.