

Приложение № 1

к приказу Директора МБОУ СОШ
д.Султанбеково МР Аскинский район РБ

от «21» 11 2018 г. № 880Д

**Правила
обработки, хранения и уничтожения персональных данных**

1. Общие положения

1.1. Настоящие Правила обработки, хранения и уничтожения персональных данных (далее – Правила) разработаны в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»,

1.2. Настоящие Правила определяют правила обработки персональных данных; сроки обработки и хранения персональных данных, порядок их уничтожения, ответственность должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных в МБОУ СОШ д.Султанбеково МР Аскинский район РБ (далее - Оператор).

1.3. Организацию работ по осуществлению обработки и защиты персональных данных, осуществлению контроля за соблюдением требований законодательства по персональным данным и локальных актов Оператора осуществляет Ответственный за организацию обработки персональных данных.

1.4. Текущий контроль за соблюдением правил по обработке персональных данных без использования средств автоматизации осуществляет Ответственный за организацию обработки персональных данных.

1.5. Настоящие Правила не исключают обязательного выполнения других руководящих документов по вопросам обработки, передачи, хранения и уничтожения персональных данных.

1.6. Должностные лица, допустившие нарушения требований руководящих и нормативных документов по вопросам защиты персональных данных, привлекаются к ответственности в соответствии с законодательством Российской Федерации.

2. Основные понятия

2.1. В настоящих Правилах используются следующие основные понятия:

персональные данные - любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу;

обработка персональных данных - любое действие (операция) или совокупность действий, 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;

автоматизированное рабочее место (АРМ) — программно-технический комплекс автоматизированной системы, предназначенный для автоматизации деятельности определенного вида;

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

конфиденциальность персональных данных - обязательное для соблюдения назначенным ответственным лицом, получившим доступ к персональным данным, требование не допускать их распространения без согласия субъекта или иного законного основания;

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

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

блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

носитель - материальный объект, в том числе физическое поле, в котором информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

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 становится невозможно 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;

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

3. Общие требования к обработке персональных данных

3.1. Обработке подлежат только те персональные данные, которые отвечают целям их обработки.

3.2. Сотрудники Оператора и иные лица, получившие доступ к персональным данным, не вправе раскрывать третьим лицам и распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

3.3. Персональные данные не могут быть использованы в целях причинения имущественного и (или) морального вреда гражданам, затруднения реализации прав и свобод граждан.

3.4. Согласие на обработку персональных данных подписывается субъектом персональных данных собственноручно, либо его законным представителем. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного электронной подписью в соответствии с федеральным законодательством.

3.5. Необходимо получить согласие субъекта персональных данных на обработку его персональных данных (за исключением случаев, предусмотренных федеральными законами):

- при передаче персональных данных третьим лицам;
- при распространении персональных данных,
- при принятии решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, на основании исключительно автоматизированной обработки его персональных данных.

3.6. Обязанность получения письменного согласия на обработку персональных данных субъекта персональных данных возлагается на отдел кадров Оператора.

3.7. Оператор не вправе запрашивать у субъектов информацию об их расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни.

4. Порядок обработки персональных данных в информационной системе персональных данных

4.1. В информационной системе персональных данных должна соблюдаться парольная защита.

4.2. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4.3. Все машинные носители информации, на которых записана информация, содержащая персональные данные субъектов, должны быть зарегистрированы в «Журнале учета машинных носителей информации», и иметь этикетку, на которой указывается учетный (регистрационный) номер.

4.4. При эксплуатации информационной системы, предназначенной для обработки персональных данных, пользователям запрещается:

- вносить изменения в состав, конструкцию, конфигурацию и размещение технических средств информационной системы;
- вносить изменения в состав программного обеспечения, структуру файловой системы;
- осуществлять попытки несанкционированного доступа к ресурсам информационной системы и к информации других пользователей;
- подключать информационную систему персональных данных к информационным сетям общего пользования без использования дополнительных средств защиты (сертифицированные межсетевые экраны и средства криптографической защиты данных);

- использовать неучтенные машинные накопители информации.

4.5. При проведении технического обслуживания и ремонта компонентов информационной системы персональных данных, запрещается передавать указанные компоненты третьим лицам в отсутствие пункта о соблюдении конфиденциальности в соглашении, заключенном с этими лицами.

4.6. Обязанности сотрудника по обработке ПДн в информационной системе персональных данных:

- при работе с АРМ использовать только установленное программное обеспечение, необходимое для выполнения должностных обязанностей сотрудника;
- при обработке персональных данных на АРМ исключить возможность ознакомления посторонних лиц с электронными документами;
- при отлучении с рабочего места закрывать все электронные документы, базы данных, содержащие персональные данные, блокировать АРМ;
- использовать только учтенные машинные носители информации;
- обеспечивать сохранность машинных носителей информации;
- при повреждении и выходе из строя внешних машинных носителей сдавать их для уничтожения;
- докладывать непосредственному руководителю о выявленных или допущенных нарушениях правил.

5. Порядок обработки персональных данных без использования средств автоматизации

5.1. Персональные данные при их обработке без использования средств автоматизации, фиксируются на отдельных носителях персональных данных, в специальных разделах или на полях форм (бланков).

5.2. При фиксации персональных данных на носителях не допускается фиксация на одном носителе персональных данных, цели обработки которых заведомо не совместимы.

5.3. При использовании типовых форм документов, характер информации в которых предполагается включение в них персональных данных, должно соблюдаться следующее условие: типовая форма или связанные с ней документы (административный регламент, 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, 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.

5.4. В отношении каждой категории персональных данных должны быть определены места хранения персональных данных (носителей персональных данных) и установлен перечень должностей, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным.

3.5. Обязанности сотрудника по обработке ПДн без использования средств автоматизации:

- выполнять требования, установленные Правилами обработки, хранения и уничтожения персональных данных и Политикой обработки и защиты персональных данных;
- обеспечить сохранность бумажных документов в процессе обработки и хранения;
- исключать просмотр документов, содержащих персональные данные, третьими лицами, в том числе сотрудниками Оператора, которым не предоставлен доступ к личным документам;
- хранить документы на рабочем месте исключительно с целью обработки ПДн. При достижении целей обработки сдавать документы в архив, либо осуществлять в установленном порядке уничтожение документов;
- в нерабочее время бумажные документы хранить в запираемых секциях рабочих столов или в шкафах, либо в запираемом помещении.

6. Порядок и срок хранения персональных данных

6.1 Хранение персональных данных должно осуществляться не дольше, чем этого требуют цели обработки персональных данных, если иной срок хранения персональных данных не установлен федеральным законом, иным нормативным правовым документом или договором, стороной которого, является субъект персональных данных.

6.2 Съёмные машинные носители персональных данных должны храниться в сейфах (металлических шкафах), оборудованных внутренними замками с двумя или более дубликатами ключей и приспособлениями для опечатывания замочных скважин или кодовыми замками. В случае если на съёмном машинном носителе персональных данных хранятся только персональные данные в зашифрованном с использованием СКЗИ виде, допускается хранение таких носителей вне сейфов (металлических шкафов).

6.3 Конкретные сроки хранения персональных данных указываются в номенклатуре дел.

6.4 Срок хранения персональных данных в электронном виде не может превышать срока хранения персональных данных на бумажных носителях.

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

6.6 Места хранения носителей персональных данных определяются распоряжением Директора.

6.7 Ответственный за организацию обработки персональных данных осуществляет контроль за хранением и использованием носителей персональных данных с целью исключения несанкционированного использования, изменения, распространения и уничтожения персональных данных, находящихся на этих носителях.

6.8 Вынос носителей персональных данных за пределы помещения Оператора допускается исключительно по служебной необходимости с разрешения непосредственного руководителя.

7. Передача персональных данных

7.1 Передача персональных данных третьим лицам возможна при соблюдении следующих условий:

7.1.1 Наличие письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, установленных федеральными законами.

7.1.2 Соблюдение лицами, получающими персональные данные субъекта, режима конфиденциальности персональных данных.

7.2 Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора. Лицо, осуществляющее обработку персональных данных по поручению Оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом о персональных данных. В поручении должны быть определены: перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии с Федеральным законом о персональных данных.

7.3 Трансграничная передача персональных данных, обрабатываемых в Операторе, допускается в случаях, предусмотренных Федеральным Законодательством и международными договорами Российской Федерации.

7.4 Оператор передает персональные данные субъекта персональных данных третьим лицам на основании письменного запроса о предоставлении персональных данных (далее - запрос). Запрос должен содержать сведения о положениях федерального закона, устанавливающего право обратившегося на получение запрашиваемых персональных данных или о заключенном договоре (соглашении) об информационном взаимодействии с Оператором; о целях получения персональных данных; о составе персональных данных. В случае если запрос направляется по информационно-телекоммуникационным сетям, он должен быть подписан усиленной квалифицированной электронной подписью.

8. Доступ к персональным данным

8.1 Перечень должностей, допущенных к обработке персональных данных, утверждается распоряжением Директора.

8.2 В отношении отдельных категорий персональных данных возможно ограничение допуска сотрудников, занимающих одну должность, к обработке персональных данных, на основании распоряжения Директора.

8.3 Сотрудник, получивший доступ к персональным данным, обязан не предоставлять третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральными законами.

8.4 Сотрудник, допущенный к обработке персональных данных, принимает на себя обязательство в случае прекращения с ним трудовых отношений, перевода на другую работу, освобождения от работ, связанных с обработкой персональных данных, прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей. Обязательство в письменной форме доводится до личного дела сотрудника.

8.5 Сотрудники, допущенные к обработке персональных данных, должны быть информированы о характере обработки, категориях обрабатываемых персональных данных, а также об особенностях и условиях осуществления такой обработки.

8.6 Субъект персональных данных, чьи персональные данные обрабатываются работодателем, имеет право на доступ к своим персональным данным в соответствии со статьей 14 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

9. Порядок уничтожения персональных данных

9.1 Обрабатываемые персональные данные подлежат уничтожению, либо уничтожению по окончании срока хранения бумажных носителей персональных данных, достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством.

9.2 Уничтожение персональных данных осуществляется комиссией с составлением акта, по истечению сроков хранения и обработки персональных данных.

9.3 Уничтожение бумажных носителей персональных данных должно осуществляться путем сожжения, либо измельчения в бумаго-уничтожающей машине.

9.4 При необходимости уничтожения части персональных данных, уничтожается материальный носитель с предварительным копированием сведений, подлежащих уничтожению, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению.

9.5 Уничтожение машинных носителей информации должно производиться следующими способами:

- оптические диски и дискеты – путем физического повреждения;
- флеш накопители – путем ударно-механического повреждения основной платы, на которой располагается флеш память;
- накопитель на жестком магнитном диске – путем измельчения магнитных данных.

9.6 Для удаления персональных данных с машинных носителей информации могут использоваться программные методы гарантированного удаления информации, в которых используются алгоритмы гарантированного удаления данных.

10. Для удаления персональных данных из электронных баз данных используются методы обезличивания персональных данных с целью невозможности определить принадлежность персональных данных конкретному субъекту в соответствии с Правилами работы с обезличенными данными.

11. Ответственность за неисполнение (ненадлежащее исполнение) настоящих Правил

11.1. Сотрудники несут ответственность за ненадлежащее исполнение или неисполнение настоящих Правил в соответствии с действующим законодательством Российской Федерации и локальными актами Оператора.