РАССМОТРЕНО И СОГЛАСОВАНО
на заседании Управляющего совета
протокол № 2
от «31» 08 2020г.

УТВЕРЖДАЮ
Директор МАОУ «СОШ № 15»
городского округа г. Стерлитамак
_____ И.Ф. Шарипов
Ввести в действие
приказ № 308 от «01» 09 2020г.

ПРАВИЛА
обработки, хранения и уничтожения персональных данных в МАОУ «СОШ № 15» городского округа г. Стерлитамак РБ

1. Общие положения

1.1. Настоящие Правила обработки, хранения и уничтожения персональных данных (далее – Правила) в МАОУ «СОШ № 15» (далее – Оператор, Организация) разработаны в соответствии с Федеральным законом от 27.07.2006 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 15.09.2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», а также иными нормативными документами по защите персональных данных.

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

1.3. Общая ответственность за организацию обеспечения защиты персональных данных возлагается на ответственного за обеспечение безопасности персональных данных.

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

1.5. По фактам и попыткам несанкционированного доступа к персональным данным, а также случаям утечки персональных данных или утрат машинных носителей информации (далее – МНИ) с персональных данных проводятся служебные расследования.

1.6. При передаче персональных данных по каналам связи, выходящим за пределы контролируемой зоны и незащищенным от несанкционированного

доступа, обязательно использование средств защиты, прошедших процедуру оценки соответствия.

1.7. В настоящих Правилах используются следующие основные понятия.

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

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

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

Автоматизированная обработка ПДн – обработка ПДн с помощью средств вычислительной техники.

Распространение ПДн – действия, направленные на раскрытие ПДн неопределенному кругу лиц.

Предоставление ПДн – действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц.

Уничтожение ПДн – действия, в результате которых становится невозможным восстановить содержание ПДн в ИСПДн и (или) в результате которых уничтожаются материальные носители ПДн.

Обезличивание ПДн – действия, в результате которых становится невозможным, без использования дополнительной информации, определить принадлежность ПДн конкретному субъекту ПДн.

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

2. Общие требования к обработке ПДн.

2.1.Обработке подлежат только ПДн, которые отвечают целям их обработки.

2.2.Операторы и иные лица, получившие доступ к ПДн, обязаны не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом.

3. Порядок обработки ПДн с использованием средств автоматизации.

3.1. Ответственность за обеспечение защиты ПДн в информационной системе, возлагается на ответственного лица за обеспечение безопасности ПДн.

3.2. Допуск к работе в ИСПДн осуществляется после ввода её в эксплуатацию в составе информационной системы, предназначенных для обработки ПДн.

3.3. В ИСПДн должна соблюдаться парольная защита.

3.4. Не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.

3.5. Все машинные носители информации, на которых записана информация, содержащая ПДн субъектов, должны быть зарегистрированы по «Журналу учета машинных носителей» (Приложение №1), и иметь этикетку, на которой указывается учетный (регистрационный) номер.

3.6. При эксплуатации информационной системы, предназначенной для обработки ПДн, пользователям **запрещается**:

- вносить изменения в состав, конструкцию, конфигурацию и размещение технических средств информационной системы;
- вносить изменения в состав программного обеспечения, структуру файловой системы без письменного разрешения ответственного лица за обеспечение безопасности ПДн;
- осуществлять попытки несанкционированного доступа к резервам информационной системы и к информации других пользователей;
- подключать ИСПДн к информационным сетям общего пользования без использования дополнительных средств защиты (сертифицированные межсетевые экраны и средства криптографической защиты данных);
- использовать неучтенные машинные накопители информации.

3.7. При возникновении сбоев в работе ИСПДн, появления программ-вирусов немедленно сообщить ответственному лицу за администрирование информационных систем или ответственному за обеспечение безопасности ПДн.

3.8. При проведении технического обслуживания и ремонта ИСПДн, запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения ПДн. Вышедшие из строя элементы и блоки заменяются на исправные.

4. Обязанности работника по обработке ПДн с использования средств автоматизации:

4.1. При работе с персональным компьютером использовать только установленное программное обеспечение, необходимое для выполнения должностных обязанностей работника.

4.2. Хранить парольную информацию в тайне.

4.3. При обработке ПДн на персональном компьютере, исключить возможность ознакомления с электронными документами посторонних лиц. При отлучении с рабочего места закрывать все электронные документы, базы данных, содержащие ПДн, блокировать рабочую станцию.

4.4. Использовать только учтенные внешние электронные носители информации, промаркированные и зарегистрированные ответственным лицом за обеспечение безопасности ПДн (flash-накопители, компакт-диски, дискеты и др.).

4.5. В случае необходимости более чем однократного использования электронных носителей информации, полученных из сторонних организаций, учитывать электронные носители в журнале учета электронных носителей. В случае однократного использования электронного носителя для переноса информации с носителя в ИСПДн передавать ответственному лицу за обеспечение безопасности ПДн носители для уничтожения.

4.6. В нерабочее время внешние электронные носители, содержащие ПДн, хранить в запирающихся на ключ секциях рабочих столов или в металлических шкафах.

4.7. При достижении целей обработки ПДн, повреждении и выходе из строя носителей сдавать учтенные электронные носители ПДн для уничтожения ответственному лицу за обеспечение безопасности ПДн.

4.8. Докладывать непосредственному руководителю о нарушениях правил безопасности.

5. Порядок обработки ПДн без использования средств автоматизации.

5.1. ПДн при их обработке без использования средств автоматизации, фиксируются на отдельных материальных носителях ПДн (далее – материальные носители), в специальных разделах или на полях форм (бланков).

5.2. При фиксации ПДн на материальных носителях не допускается фиксация на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы.

5.3. При использовании типовых форм документов, характер информации в

которых предполагается включение в них ПДн (далее – типовая форма), должно соблюдаться следующее условие:

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки ПДн, осуществляемой без использования средств автоматизации, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта ПДн, источник получения ПДн, сроки обработки ПДн, перечень действий с ПДн, которые будут совершаться в процессе их обработки, общее описание используемых Оператором способов обработки ПДн.

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

6. Обязанности работника по обработке ПДн без использования средств автоматизации:

6.1. Выполнять требования по обеспечению режима конфиденциальности проводимых работ, установленные Правилами обработки, хранения и уничтожения ПДн и Положением об организации и обеспечении защиты ПДн Оператора.

6.2. Обеспечить сохранность бумажных документов в процессе обработки и хранения.

6.3. В рабочее время исключать просмотр вверенных документов посторонними людьми, а также работниками Оператора, которым не предоставлен доступ к ПДн.

6.4. Использовать документы, содержащие ПДн, только в рамках должностных обязанностей.

6.5. Хранить документы на рабочем месте исключительно с целью обработки ПДн. При достижении целей работы с документами сдавать документы в архив либо осуществлять уничтожение документов с использованием средств уничтожения бумажных носителей.

6.6. В нерабочее время бумажные документы хранить в секциях рабочих столов или в шкафах (либо сдавать все помещение под охрану).

7. Порядок хранения ПДн.

7.1. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к

ним доступ.

7.2. Необходимо обеспечивать раздельное хранение ПДн (материальных носителей), обработка которых осуществляется в различных целях.

7.3. Машинные носители информации ПДн в нерабочее время должны храниться в сейфах или несгораемых шкафах у должностных лиц, уполномоченных на обработку ПДн.

7.4. Должностным лицам, уполномоченным на обработку ПДн, запрещается:

- хранить машинные носители информации на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам без разрешения руководителя подразделения;
- делать несанкционированные копии с носителей ПДн;
- выносить носители с ПДн за пределы Организации.

8. Передача ПДн

8.1. При передаче ПДн субъекта Оператор должен соблюдать следующие требования:

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

8.1.2. Обработка ПДн субъектов в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только с его предварительного согласия.

8.1.3. Предупредить лиц, получивших ПДн 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, получившие ПДн субъекта, обязаны соблюдать режим конфиденциальности. Данное Положение не распространяется на обмен ПДн субъектов в порядке, установленном федеральными законами.

8.1.4. Оператор вправе поручить обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта. Лицо, осуществляющее обработку ПДн по поручению Оператора, обязано соблюдать принципы и правила обработки ПДн, предусмотренные Федеральным законом о ПДн. В поручении оператора должны быть

определены перечень действий (операций) с ПДн, которые будут совершаться лицом, осуществляющим обработку ПДн, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность ПДн и обеспечивать безопасность ПДн при их обработке, а также должны быть указаны требования к защите обрабатываемых ПДн в соответствии с Федеральным законом о ПДн. Разрешать доступ к ПДн субъектов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те ПДн работника, которые необходимы для выполнения конкретной функции.

8.1.5. Не запрашивать у субъектов информацию об их расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни.

8.1.6. Передавать ПДн работников представителям в порядке, установленном Трудовым кодексом Российской Федерации, и ограничивать эту информацию только теми ПДн субъекта, которые необходимы для выполнения указанными представителями их функции.

9 Доступ к ПДн

9.1 Перечень лиц, имеющих право доступа к ПДн, определяется документом «Список категорий лиц, допущенных к обработке ПДн», утверждённым внутренним локальным актом.

9.2 Субъект ПДн, чьи ПДн обрабатываются в информационной системе имеет право:

9.2.1 Получать доступ к своим ПДн и ознакомление с ними, включая право на безвозмездное получение копий любой записи, содержащей ПДн этого субъекта.

9.2.2 Требовать от Оператора уточнения, исключения или исправления неполных, неверных, устаревших, недостоверных, незаконно полученных или не являющих необходимыми для оператора ПДн.

9.2.3 Получать от Оператора:

- сведения о лицах, которые имеют доступ к ПДн или которым может быть предоставлен такой доступ;
- перечень обрабатываемых ПДн и источник их получения;
- сроки обработки ПДн, в том числе сроки их хранения;
- сведения о том, какие юридические последствия для субъекта ПДн может повлечь за собой обработка его ПДн.

9.2.4 Требовать извещения Оператором всех лиц, которым ранее были сообщены неверные или неполные ПДн, обо всех произведенных в них исключениях, исправлениях или дополнениях.

9.2.5 Копировать и делать выписки ПДн субъекта разрешается исключительно в служебных целях с письменного разрешения руководителя Организации.

9.3 Передача информации третьей стороне возможна только при письменном согласии субъектов.

10. Контроль и надзор за выполнением требований настоящего Положения

Контроль и надзор за выполнением требований настоящего Положения осуществляется в соответствии с документом «Правила проведения внутренних проверок режима защиты ПДн».

Контроль заключается в проверке выполнения требований нормативных документов по защите информации, а также в оценке обоснованности и эффективности, принятых мер. Он может проводиться ответственным за организацию обработки ПДн (или ответственным за обеспечение безопасности ПДн), или на договорной основе сторонними организациями, имеющими лицензии на деятельность по технической защите конфиденциальной информации.

11. Финансирование мероприятий по обеспечению безопасности ПДн

Финансирование производится из средств Оператора.

12. Ответственность за нарушение требований настоящего положения

Лица, виновные в нарушении требований настоящего Положения, несут гражданскую, уголовную, административную, дисциплинарную и иную ответственность, предусмотренную законодательством Российской Федерации.

13. Порядок уничтожения ПДн.

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

13.2.Уничтожение ПДн осуществляется комиссией с составлением акта уничтожения материальных носителей ПДн, по истечению сроков хранения и обработки ПДн.

13.3.Уничтожение бумажных носителей ПДн осуществляется путем

сожжения, либо измельчения в бумаго-уничтожающей машине.

13.4.При необходимости уничтожения части ПДн, уничтожается материальный носитель с предварительным копированием сведений, не подлежащих уничтожению, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению.

13.5.Уничтожение машинных носителей информации производится следующим путем:

- оптические диски и дискеты – путем оплавления в бесформенную массу;
- флеш-накопители – путем ударно-механического повреждения основной платы, на которой располагается флеш память;
- накопитель на жестком магнитном диске – путем ударно-механического повреждения исключения возможности восстановления информации в лабораторных условиях.

13.6.Для удаления информации с машинных носителях информации могут использоваться программные методы гарантированного удаления информации, в которых используются основные алгоритмы гарантированного удаления данных.

13.7.Для удаления информации, содержащей ПДн, из электронных баз данных применяется метод обезличивания ПДн с целью невозможности определить принадлежность ПДн конкретному субъекту.

Работнику запрещается:

1) Разглашать ПДн в беседах с посторонними лицами, а также с работниками, если этого не требуется для исполнения им своих служебных обязанностей.

2) Выносить носители ПДн (в том числе бумажные документы) за пределы помещений, если это не связано с выполнением должностных обязанностей работника

3) Передавать ПДн по незащищенным каналам связи (в том числе, с использованием общедоступных почтовых серверов типа mail.ru, yandex.ru и прочих).

4) Размещать и хранить ПДн на ресурсах, не предусмотренных технологическим процессом обработки ПДн в ИСПДн (в том числе, сетевых дисках, разделяемых папках, папках Exchange, а также локальных накопителях и жестких дисках компьютера) Подключать к техническим средствам ИСПДн нештатные устройства ввода-вывода.

5) Использовать неучтенные внешние электронные носители информации.

6) Использовать поступающие из сторонних организаций внешние электронные носители информации без предварительной проверки их на наличие вирусов. При обнаружении на носителе зараженного и не

поддающегося лечению файла дальнейшее использование носителя не допускается.

7) Запускать и выполнять посторонние прикладные программы, не предусмотренные технологией работы на компьютере.

8) Обрабатывать ПДн в случае сбоев в работе средств защиты информации.

9) Использовать ресурсы Интернет (осуществлять обмен сообщениями электронной почты) в случае сбоев в работе средств антивирусной защиты.

14. Ответственность за нарушение безопасности при обработке ПДн в ИСПДн

14.1.Правила является локальным правовым актом, обязательным для выполнения работниками, допущенными к обработке ПДн.

14.2.На работника возлагается персональная ответственность за невыполнение и/или нарушение требований и положений, установленных настоящими Правилами.

14.3.Работник несет ответственность за сохранность в процессе обработки ПДн, к которым ему разрешен доступ, за сохранность и работоспособное состояние технических, программных средств, носителей ПДн (в том числе бумажных документов), используемых им в работе.

Приложение №1

Журнал учета машинных носителей информации

Дата, регистрационный номер	Шифр заказа, задачи, учетный номер, откуда поступил	Тип машинного носителя информации, машинного документа	Количество экземпляров	Номер экземпляра	Количество в экземпляре (штук, лент, листов)	Расписка в получении (ф.и.о., подпись, дата), отметка об отправке	Расписка в обратном приеме (ф.и.о., подпись, дата)	Место хранения машинного носителя информации, машинного документа	Отметка об уничтожении (складировании в урну) бракованных машинных носителей информации, машинных документов (подпись, дата)	Отметка об уничтожении машинных носителей информации, машинных документов, стирании информации (номер и дата акта)