УТВЕРЖДАЮ

Директор МБОУ “Школа №17”
_____ Е.В.Круглова
приказ №98 от 06.04.2021

Положение о защите персональных данных муниципального бюджетного общеобразовательного учреждения города Ростова-на-Дону “Школа №17”

1. Общие положения

1.1. Настоящее Положение о защите персональных данных (далее – Положение) МБОУ “Школа №17”(далее – Учреждение, либо оператор) разработано во исполнение Политики в отношении обработки персональных данных (далее Политика) на основании Конституции Российской Федерации, Трудового кодекса Российской Федерации, Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных" и других нормативно-правовых актов Российской Федерации.

1.2. Настоящее Положение устанавливает порядок приема, получения, поиска, сбора, систематизации, накопления, хранения, уточнения, обновления, изменения, использования, распространения (в том числе передачи), обезличивания, блокирования, уничтожения, учета документов, содержащих сведения, отнесенные к персональным данным субъектов персональных данных Учреждения, с использованием средств автоматизации или без использования таких средств.

1.3. Целью настоящего Положения является защита персональных данных субъектов персональных данных Учреждения от несанкционированного доступа и разглашения, неправомерного их использования или утраты. Персональные данные являются конфиденциальной, строго охраняемой информацией.

1.4. Основные термины и определения, применяемые в настоящем Положении:

1.4.1. **Персональные данные** - любая информация, относящаяся к определенному 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, определяемая нормативно-правовыми актами Российской Федерации в области трудовых отношений и Уставной деятельностью Учреждения.

1.4.2. **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.

1.4.3. **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.

1.4.4. **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.

1.4.5. **Блокирование персональных данных** — временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

1.4.6. **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.

1.4.7. **Обезличивание персональных данных** — действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

1.4.8. **Информационная система персональных данных** - 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.

1.4.9. **Конфиденциальность персональных данных** - обязательное для соблюдения Учреждением или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Обеспечения конфиденциальности персональных данных не требуется:

- в случае обезличивания персональных данных;
- в отношении общедоступных персональных данных.

1.4.10. **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.

В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных (Приложение 5) могут включаться фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные данным субъектом.

Сведения о субъекте персональных данных могут быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта или по решению ректора Учреждения, либо по решению суда или иных уполномоченных государственных органов.

1.4.11. **Трансграничная передача персональных данных** – передача персональных данных через государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

1.4.12. **Работники** - лица, состоящие в трудовых отношения с Учреждением, либо претенденты на открытые вакантные должности, вступившие в правоотношения по вопросу приема на работу.

1.4.13. **Оператор** — юридическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели и содержание обработки персональных данных.

1.5. **К субъектам персональных данных** Учреждения (далее – субъекты) относятся лица – носители персональных данных, передавшие свои персональные данные оператору (как на добровольной основе, так и в рамках выполнения требований нормативно-правовых актов) для приема, получения, поиска, сбора, систематизации, накопления, хранения, уточнения, обновления, изменения, использования, распространения (в том числе передачи), обезличивания, в том числе:

- работники оператора, бывшие работники, кандидаты на замещение вакантных должностей;
- лица, имеющие договорные отношения гражданско-правового характера с оператором;
- учащиеся, воспитанники образовательных учреждений Пролетарского района, их родители (законные представители);
- руководители и работники образовательных учреждений Пролетарского района;
- контрагенты Оператора (физические лица), представители и работники контрагентов Оператора (юридических лиц), участники закупок товаров, работ и услуг для обеспечения государственных и муниципальных нужд Оператора;
- получатели муниципальных услуг в соответствии с уставной деятельностью Оператора;
- физические лица, обратившиеся к Оператору в порядке, установленном Федеральным законом "О порядке рассмотрения обращений граждан Российской Федерации".

1.6. Персональные данные защищаются от несанкционированного доступа в соответствии с нормативно-правовыми актами Российской Федерации, нормативно-распорядительными актами и рекомендациями регулирующих органов в области защиты информации, а также утвержденными регламентами и инструкциями Учреждения.

1.7. Сбор, хранение, использование и распространение персональных данных лица без письменного его согласия не допускаются. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении срока хранения, установленных законодательством Российской Федерации.

1.8. Должностные лица Учреждения, в обязанности которых входит ведение персональных данных субъектов персональных данных, обязаны обеспечить каждому субъекту возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

1.8. Персональные данные не могут быть использованы в целях:

- причинения имущественного и морального вреда гражданам;
- затруднения реализации прав и свобод граждан Российской Федерации.

1.9. Настоящее Положение и изменения к нему утверждаются начальником отдела образования; являются обязательным для исполнения всеми работниками, имеющими доступ к персональным данным субъектов персональных данных Учреждения.

Работники Учреждения до заключения трудового договора должны быть ознакомлены под роспись с настоящим Положением в редакции, действующей на

момент ознакомления. Факт ознакомления удостоверяется проставлением подписи непосредственно в трудовом договоре.

2. Принципы обработки персональных данных

2.1. Обработка персональных данных в Учреждении осуществляется на основе следующих принципов:

- законности целей и способов обработки персональных данных и добросовестности;
- соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Учреждения;
- соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- недопустимости объединения, созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

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

2.3. Субъект персональных данных является собственником своих персональных данных и самостоятельно решает вопрос передачи Учреждению своих персональных данных.

2.4. Держателем персональных данных является Учреждение, которой субъект персональных данных добровольно передает во владение свои персональные данные. Учреждение выполняет функцию владения этими данными и обладает полномочиями распоряжения ими в пределах, установленных законодательством.

2.5. Получение, хранение, передача или любое другое использование персональных данных субъекта персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников и обучающихся, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

3. Понятие и состав персональных данных

3.1. Под персональными данными субъектов персональных данных понимается информация, необходимая Учреждению в связи с трудовыми отношениями или уставной деятельностью и касающаяся конкретного субъекта персональных данных, позволяющие идентифицировать его личность. Персональные данные являются конфиденциальной информацией.

3.2. К персональным данным относятся:

- фамилия, имя, отчество; дата (день, месяц, год) и место рождения;
- адрес регистрации и адрес фактического проживания;
- контактная информация (телефон, адрес электронной почты);
- семейное положение;
- состав семьи;

- образование; специальность, профессия;
- занимаемая должность;
- сведения о трудовом и общем стаже;
- сведения о заработной плате работника, иных выплатах субъектам персональных данных;
- сведения о социальных льготах;
- сведения, содержащиеся в документах:

1. паспорт или иное удостоверение личности;
2. страховое свидетельство обязательного пенсионного страхования;
3. воинского учета;
4. свидетельство о постановке на учет в налоговом органе, содержащее сведения об идентификационном номере налогоплательщика;

- об образовании, профессиональной переподготовке, повышении квалификации, стажировки;
- анкеты (резюме), автобиографии, заполняемые субъектами персональных данных (в том числе - сведения о перемене фамилии, наличии детей и иждивенцев, знание иностранных языков);
- иные документы, которые с учетом специфики работы и в соответствии с законодательством Российской Федерации должны быть предъявлены при заключении трудового договора или в период его действия;
- трудовой договор и соглашения к нему;
- кадровые приказы (о приеме, переводе, увольнении и иные приказы);
- основания к приказам по личному составу;
- личные дела, личные карточки (форма Т-2);
- трудовые книжки работников;
- результаты медицинского обследования;
- об аттестации, собеседовании, повышении квалификации, результатах оценки и обучения;

- фотография;
- иные сведения, которые необходимы для корректного документального оформления правоотношений между субъектом персональных данных и Учреждением.

4. **Получение, обработка и хранение персональных данных**

4.1. Учреждение получает сведения о персональных данных субъектов персональных данных из следующих документов:

4.1.1. При решении вопросов, связанных с трудовыми отношениями:

- паспорт или иной документ, удостоверяющий личность;
- трудовая книжка;
- страховое свидетельство государственного пенсионного страхования;
- свидетельство о постановке на учет в налоговом органе, содержащее сведения об идентификационном номере налогоплательщика;
- документы воинского учета, содержащие сведения о воинском учете военнообязанных и лиц, подлежащих призыву на военную службу;
- документ об образовании, о квалификации или о наличии специальных знаний или специальной подготовки, содержащий сведения об образовании, профессии;
- иные документы и сведения, представляемые субъектом персональных данных при приеме на работу, а также в процессе работы.

4.1.2. При оказании услуг гражданско-правового характера, а также договорных отношений с контрагентами (физическими лицами):

- паспорт или иной документ, удостоверяющий личность;
- страховое свидетельство государственного пенсионного страхования;
- свидетельство о постановке на учет в налоговом органе, содержащее сведения об идентификационном номере налогоплательщика;
- иные документы, предусмотренные законодательством Российской Федерации.

4.1.3. При реализации мероприятий по направлениям уставной деятельности:

- паспорт или иной документ, удостоверяющий личность;
- трудовая книжка;
- страховое свидетельство государственного пенсионного страхования;
- свидетельство о постановке на учет в налоговом органе, содержащее сведения об идентификационном номере налогоплательщика;
- документы воинского учета, содержащие сведения о воинском учете военнообязанных и лиц, подлежащих призыву на военную службу;
- документ об образовании, о квалификации или о наличии специальных знаний или специальной подготовки, содержащий сведения об образовании, профессии;
- свидетельство о рождении (для лиц, не достигших 14 летнего возраста);
- иные документы и сведения, представляемые субъектом персональных данных при приеме на работу, в процессе работы, а также предусмотренные законодательством Российской Федерации.

Субъект персональных данных обязан представлять Учреждению достоверные сведения о себе. Оператор имеет право проверять достоверность указанных сведений в порядке, не противоречащим законодательству России.

4.2. Обработка персональных данных субъекта персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия в трудоустройстве, обучении, регулирования трудовых отношений, уставной деятельности Учреждения, обеспечения личной безопасности, контроля количества и качества выполняемой работы, обеспечения сохранности имущества и иных целей, отраженных в Политике.

4.3. При определении объема и содержания, обрабатываемых персональных данных субъектов Оператор руководствуется Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, законодательством в сфере образования и иными федеральными законами.

4.4. Все персональные данные субъекта персональных данных оператор получает непосредственно у указанных субъектов. Работник, обеспечивающий обработку персональных данных, принимает от субъекта документы, проверяет их полноту и правильность указываемых сведений.

4.5. Если персональные данные субъекта персональных данных возможно получить исключительно у третьей стороны, то субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие .Оператор должен 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...

4.6. Условием обработки персональных данных субъекта персональных данных является его письменное согласие. Письменное согласие субъекта на обработку его персональных данных должно включать в себя:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

- наименование и адрес оператора персональных данных;

- цель обработки персональных данных;

- перечень персональных данных, на обработку которых дается согласие субъекта;

- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Учреждением способов обработки персональных данных;

- срок, в течение которого действует согласие, а также порядок его отзыва.

Согласие на обработку персональных данных может быть отозвано субъектом персональных данных.

4.7. Согласия субъекта на обработку его персональных данных не требуется в следующих случаях:

- обработка персональных данных осуществляется на основании федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;

- обработка персональных данных осуществляется для статистических или иных целей при условии обязательного обезличивания персональных данных;

- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта, если получение его согласия при данных обстоятельствах невозможно;

- обработка персональных данных необходима для доставки почтовых отправлений организациями почтовой связи, для осуществления операторами электросвязи расчетов с пользователями услуг связи за оказанные услуги связи, а также для рассмотрения претензий пользователей услугами связи;

- осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами.

4.8. Для обработки персональных данных, содержащихся в согласии в письменной форме субъекта на обработку его персональных данных, дополнительное согласие не требуется.

4.9. В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных в письменной форме дает его законный представитель.

4.10. В случае, если Учреждение на основании договора поручает обработку персональных данных другому лицу, существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке.

4.11. Оператор не имеет права получать и обрабатывать персональные данные субъекта о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной, частной жизни, за исключением, если:

- субъект дал согласие в письменной форме на обработку своих соответствующих персональных данных;

- персональные данные являются общедоступными;

- персональные данные относятся к состоянию здоровья субъекта и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов

либо жизни, здоровья или иных жизненно важных интересов других лиц, и получение согласия субъекта в данный момент невозможно;

- обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;

- обработка персональных данных необходима в связи с осуществлением правосудия;

- обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, а также в соответствии с уголовно-исполнительным законодательством Российской Федерации.

В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст.24 Конституции РФ работодатель вправе получать и обрабатывать данные о частной жизни субъекта только с его письменного согласия.

Обработка персональных данных, перечисленных в п.4.11. настоящего Положения должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась обработка.

4.12. Сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность (биометрические персональные данные), могут обрабатываться только при наличии согласия субъекта персональных данных в письменной форме.

4.13. Обработка биометрических персональных данных может осуществляться без согласия субъекта в связи с осуществлением правосудия, а также в случаях, предусмотренных законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, о государственной службе, о порядке выезда из Российской Федерации и въезда в Российскую Федерацию, уголовно-исполнительным законодательством Российской Федерации.

4.14. Защита персональных данных субъекта от неправомерного их использования или утраты должна быть обеспечена оператором за счет его средств в порядке, установленном федеральным законодательством РФ.

4.15. Субъекты персональных данных, и их представители должны быть ознакомлены под роспись с документами Учреждения, устанавливающими порядок обработки персональных данных, а также об их правах и обязанностях в этой области.

4.16. Документы, содержащие персональные данные работника, составляют его личное дело.

Личное дело хранится уполномоченным лицом на бумажных носителях; помимо этого, может храниться в виде электронных документов, баз данных. Личное дело пополняется на протяжении всей трудовой деятельности работника.

Письменные доказательства получения оператором согласия субъекта персональных данных на их обработку хранятся в личном деле.

4.17. При обработке персональных данных оператор вправе определять способы обработки, документирования, хранения и защиты персональных данных на базе современных информационных технологий.

4.18. Круг лиц, допущенных к работе с документами, содержащими персональные данные субъектов, определяется приказом начальником отдела образования.

4.19. Помещения, в которых хранятся персональные данные субъектов, должны быть оборудованы в установленном порядке, обеспечивающем их сохранность (надежными замками и сигнализацией на вскрытие; специально оборудованными шкафами или сейфами для хранения бумажных носителей персональных данных, находящимися в закрытом состоянии в течение рабочего дня и за его пределами).

Помещения, в которых хранятся персональные данные субъектов, в рабочее время, при отсутствии в них работников должны быть закрыты.

Проведение уборки помещений, в которых хранятся персональные данные, должно производиться в присутствии соответствующих работников.

5. **Права и обязанности сторон в области защиты персональных данных**

5.1. Субъект персональных данных обязан:

- передавать Учреждению или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен трудовым законодательством, законодательством в сфере образования, иными законодательными актами РФ, включая сведения об образовании, специальных знаниях, стаже работы, отношении к воинской обязанности, гражданстве, месте жительства и др.;
- своевременно, сообщать Учреждению об изменении своих персональных данных.

5.2. Субъект персональных данных имеет право:

5.2.1. На полную информацию о своих персональных данных и об их обработке.

5.2.2. На свободный бесплатный доступ к своим персональным данным, включая право на получение копии любой записи, содержащей персональные данные, за исключением случаев, предусмотренных действующим законодательством. Доступ к своим персональным данным предоставляется субъекту или его законному представителю Учреждением при личном обращении либо при получении запроса . Запрос должен содержать номер основного документа, удостоверяющего личность субъекта или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта или его законного представителя. Запрос может быть направлен в электронной форме и подписан электронной цифровой подписью в соответствии с законодательством Российской Федерации.

Сведения о персональных данных должны быть предоставлены субъекту персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

5.2.3. Право субъекта на доступ к своим персональным данным ограничивается в следующих случаях:

- обработка персональных данных, в том числе персональных данных, полученных в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;
- обработка персональных данных осуществляется органами, осуществляющими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если

допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

- предоставление персональных данных нарушает конституционные права и свободы других лиц.

5.2.4. Требовать от Учреждения исключения, исправления или уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также данных, обработанных с нарушением требований Трудового кодекса Российской Федерации, законодательства РФ в сфере образования и Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных». Указанное требование должно быть оформлено письменным заявлением субъекта персональных данных на имя начальника Учреждения.

5.2.5. Требовать от Учреждения извещения всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта, обо всех произведенных в них исключениях, исправлениях или дополнениях.

5.2.6. При отказе оператора исключить или исправить персональные данные субъекта, он имеет право заявить в письменной форме оператору о своем несогласии с соответствующим обоснованием такого несогласия. При отклонении оператором указанного обращения (несогласия), субъект персональных данных имеет право обжаловать действия оператора в порядке, предусмотренном законодательством России.

5.2.7. Получать информацию, касающуюся обработки его персональных данных, в том числе содержащую:

- подтверждение факта обработки персональных данных Учреждением, а также цель такой обработки;

- способы обработки персональных данных, применяемые оператором;

- сведения о должностных лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

- перечень обрабатываемых персональных данных и источник их получения;

- сроки обработки персональных данных, в том числе сроки их хранения;

- сведения о том, какие юридические последствия для него может повлечь за собой обработка его персональных данных.

5.2.8. Обжаловать в судебном порядке любые неправомерные действия или бездействие Учреждения при обработке и защите персональных данных.

5.3. Субъект персональных данных не должен отказываться от своих прав на сохранение и защиту охраняемой законом тайны.

5.4. Оператор обязан рассмотреть возражение субъекта персональных данных в течение семи рабочих дней со дня его получения и уведомить его о результатах рассмотрения такого возражения.

5.5. Если обязанность предоставления персональных данных субъектом установлена федеральным законом (включая налоговое, трудовое законодательство), оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить свои персональные данные.

5.6. Если персональные данные были получены не от субъекта (за исключением случаев, если персональные данные были предоставлены Учреждением на основании федерального закона или если персональные данные являются общедоступными), оператор до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:

1) наименование (фамилия, имя, отчество) и адрес оператора или его представителя;

2) цель обработки персональных данных и ее правовое основание;

3) предполагаемые пользователи персональных данных;

4) права субъекта в области защиты персональных данных.

5.7. Оператор обязан безвозмездно предоставить субъекту персональных данных возможность ознакомления с персональными данными, относящимися к соответствующему субъекту, а также внести в них необходимые изменения, уничтожить или блокировать соответствующие персональные данные по предоставлении субъектом сведений, подтверждающих, что персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах оператор обязан уведомить соответствующего субъекта персональных данных и третьих лиц, которым персональные данные этого субъекта были переданы .

Оператор обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по его запросу информацию, необходимую для осуществления деятельности указанного органа в установленные нормативно-правовыми актами РФ сроки.

5.8. В случае выявления недостоверных персональных данных или неправомерных действий с ними Учреждение обязано осуществить блокирование персональных данных, относящихся к соответствующему субъекту, с момента получения такой информации на период проверки. В случае подтверждения факта недостоверности персональных данных оператор на основании соответствующих документов обязан уточнить персональные данные и снять их блокирование.

5.9. В случае выявления неправомерных действий с персональными данными оператор в срок, не превышающий трех рабочих дней с даты такого выявления, обязан устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений оператор в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, обязан уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных - также указанный орган

5.10. В случае достижения цели обработки персональных данных оператор обязан незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий трех рабочих дней с даты достижения цели обработки персональных данных, если иное не предусмотрено действующим законодательством, и уведомить об этом субъекта персональных данных .

5.11. В случае отзыва субъектом согласия на обработку своих персональных данных оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением сторон и (или) федеральным законом. Об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных.

5.12. До начала обработки персональных данных Оператор обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем

намерении осуществлять обработку персональных данных, за исключением персональных данных:

- относящихся к субъектам персональных данных, которых связывают с Учреждением трудовые отношения;

- полученных Учреждением в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются Учреждением исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;

- относящихся к членам (участникам) общественного объединения или религиозной учреждения и обрабатываемых соответствующим общественным объединением или религиозной Учреждением, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов персональных данных;

- являющихся общедоступными;

- включающих в себя только фамилии, имена и отчества субъектов персональных данных;

- включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус федеральных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;

- обрабатываемых без использования средств автоматизации в соответствии с федеральными законами и иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных.

6. Доступ к персональным данным субъекта и их передача

6.1. Внутренний доступ (доступ внутри Учреждения) к персональным данным субъектов имеют работники Учреждения, которым эти данные необходимы для выполнения должностных обязанностей. Перечень должностей, при замещении которых осуществляется обработка персональных данных, утверждается начальником Учреждения и при необходимости данный перечень подлежит корректировке либо актуализации в установленном порядке.

6.2. Внешний доступ.

6.2.1. К числу массовых потребителей персональных данных вне Учреждения относятся следующие государственные и негосударственные структуры:

- налоговые органы;
- правоохранительные органы;
- органы лицензирования и сертификации;
- органы прокуратуры и ФСБ;
- органы статистики;
- учреждения, осуществляющие деятельность в сфере страхования;
- военные комиссариаты (отделы военных комиссариатов);
- органы социального страхования;
- пенсионные фонды;

- подразделения государственных и муниципальных органов управления.

6.2.2. Надзорно-контрольные органы и учреждения имеют доступ к информации исключительно в сфере своей компетенции.

6.3. Внешний доступ со стороны третьих лиц к персональным данным субъекта осуществляется с его письменного согласия, за исключением случаев, когда такой доступ необходим в целях предупреждения угрозы жизни и здоровью субъекта или других лиц, и иных случаев, установленных законодательством.

6.4. Оператор обязан сообщать персональные данные субъекта по надлежаще оформленным запросам суда, прокуратуры, иных правоохранительных органов.

6.5. Сведения о работнике или уже об уволенном работнике могут быть предоставлены в другое учреждение только на основании письменного запроса на бланке учреждения, с приложением копии заявления работника.

6.6. Персональные данные субъекта могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого субъекта персональных данных.

6.7. Передача персональных данных от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

6.8 При передаче персональных данных Оператор должен соблюдать следующие требования:

6.8.1. Не сообщать персональные данные субъекта третьей стороне без его письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта персональных данных, а также в случаях, установленных действующим законодательством.

6.8.2. Не сообщать персональные данные субъекта в коммерческих целях без его письменного согласия.

6.8.3. Предупреждать 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, обязаны соблюдать режим конфиденциальности. Данное положение не распространяется на обмен персональными данными в порядке, установленном действующим законодательством.

6.8.4. Не запрашивать информацию о состоянии здоровья субъекта, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции и возможности обучения.

6.8.5. Передавать персональные данные субъекта представителям работников и иных категорий субъектов персональных данных в порядке, установленном Трудовым кодексом Российской Федерации и Федеральным законом от 27.07.2006 № 152-ФЗ, и ограничивать эту информацию только теми персональными данными, которые необходимы для выполнения указанными представителями их функций.

6.8.6. Разрешать доступ к персональным данным исключительно специально уполномоченным лицам (при этом указанные лица должны иметь право получать лишь те персональные данные, которые необходимы для выполнения конкретных функций).

Потребители персональных данных должны подписать обязательство о неразглашении персональных данных.

6.9. Ответы на правомерные письменные запросы других предприятий, учреждений и организаций даются с разрешения начальника Учреждения в письменной форме, в том объеме, который позволяет не разглашать излишний объем персональных сведений.

6.10. Не допускается передача персональной информации по телефону.

6.11. Сведения о персональных данных передаются в письменной форме и должны иметь гриф конфиденциальности.

6.12. Трансграничная передача персональных данных в Учреждении не применяется.

7. Защита персональных данных

7.1. Комплекс мер по защите персональных данных направлен на предупреждение нарушений доступности, целостности, достоверности и конфиденциальности персональных данных и обеспечивает безопасность информации в процессе управленческой и производственной деятельности Учреждения.

7.2. Учреждение при обработке персональных данных обязано принимать необходимые организационные и технические меры, в том числе, при необходимости, использовать шифровальные (криптографические) средства для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий в соответствии с требованиями к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, требованиями к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных, установленными действующим законодательством.

7.3. Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением технологий хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения.

7.4. Мероприятия по защите персональных данных подразделяются на внутреннюю и внешнюю защиту.

7.4.1. Внутренняя защита включает следующие организационно-технические мероприятия:

7.4.1.1. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководством и специалистами Учреждения.

7.4.1.2. Для защиты персональных данных в Учреждении применяются следующие принципы и правила:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют доступа к информации, содержащей персональные данные;
- строгое избирательное и обоснованное распределение документов и информации между работниками;
- рациональное размещение рабочих мест работников, при котором исключается бесконтрольное использование защищаемой информации;
- знание работниками требований нормативных документов по защите персональных данных;
- 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 находится соответствующая вычислительная техника;

- организация порядка уничтожения информации;

- своевременное выявление нарушений требований разрешительной системы доступа сотрудниками подразделения;

- разъяснительная работа с работниками по предупреждению утраты ценных сведений при работе с конфиденциальными документами;

- защита паролями доступа персональных компьютеров, на которых содержатся персональные данные.

7.4.1.3. Личные дела работников могут выдаваться на рабочие места только начальнику Учреждения.

7.4.2. Внешняя защита включает следующие организационно-технические мероприятия:

7.4.2.1. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лиц, пытающихся совершить несанкционированный доступ и завладеть конфиденциальной информацией.

7.4.2.2. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вирусов, подмена, фальсификация содержания реквизитов документов и другое.

Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности Учреждения, посетители. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в структурных подразделениях Учреждения, использующих персональные данные.

7.4.2.3. Для защиты персональных данных осуществляется ряд мер организационно-технического характера:

- соблюдение порядка приема, учета и контроля посетителей;

- применение технических средств охраны, сигнализации;

- соблюдение требований к защите информации при интервьюировании и собеседованиях.

7.5. Порядок конкретных мероприятий по защите персональных данных с использованием или без использования электронно-вычислительной техники определяется приказами начальника, иными локальными нормативными актами.

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

8.1. Персональная ответственность является одним из главных требований к организации функционирования системы защиты персональных данных и обязательным условием обеспечения эффективности функционирования данной системы.

8.2. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

8.3. Руководитель, разрешающий доступ работника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

8.4. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством.

8.5. Каждый работник Учреждения, получающий для работы конфиденциальный документ, несет личную ответственность за сохранность носителя и конфиденциальность полученной информации.

8.6. Должностные лица, в обязанность которых входит ведение персональных данных, обязаны обеспечить каждому субъекту персональных данных, возможность ознакомления с документами и материалами, если иное не предусмотрено законом.

Неправомерный отказ в предоставлении собранных в установленном порядке персональных данных, либо несвоевременное их предоставление в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации влечет наложение на должностных лиц административного наказания в порядке, установленном действующим законодательством.

8.7. В соответствии с действующим законодательством, лица, незаконными методами получившие информацию, составляющую персональные данные, обязаны возместить причиненные убытки; такая же обязанность возлагается и на работников, не обладающих правом доступа к персональным данным.

8.8. Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения наступает в порядке, предусмотренном действующим законодательством.

8.9. Неправомерность деятельности органов государственной власти и организаций по сбору и использованию персональных данных может быть обжалована в судебном порядке.

Приложение № 2 к приказу № 98 от 06.04.2021

Угрозы безопасности персональных данных,
актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в МБОУ “Школа №17”

Обозначения и сокращения:

ИСПДн - информационная система персональных данных
ПДн - персональные данные
ПО - программное обеспечение
СЗИ - средство защиты информации
СКЗИ – система криптозащиты информации

№ п/п	Наименование угрозы
1.	Актуальные угрозы, определяемые согласно требованиям Федеральной службы по техническому и экспортному контролю
1.1.	Угроза разглашения пользовательских имен и паролей
1.2.	Просмотр (регистрация) персональных данных (далее - ПДн) с экранов дисплеев и других средств отображения графической, видео- и буквенно-цифровой информации
1.3.	Угроза нарушения конфиденциальности информации посредством ее утечки в ходе ремонта, модификации и утилизации программно-аппаратных средств
1.4.	Угроза предоставления пользователям прав доступа (в том числе по видам доступа) к ПДн и другим ресурсам информационных систем персональных данных (далее - ИСПДн) сверх объема, необходимого для работы
1.5.	Угроза неумышленного (случайного) копирования доступных ПДн на неучтенные (в том числе отчуждаемые) носители, а также печать копий документов с ПДн

1.6.	Угроза преднамеренного копирования доступных ПДн на неучтенные (в том числе отчуждаемые) носители, а также печать копий документов ПДн
1.7.	Угроза неумышленной (случайной) модификации (искажения) доступных ПДн
1.8.	Угроза преднамеренной модификации (искажения) доступных ПДн
1.9.	Угроза неумышленного (случайного) добавления (фальсификации) ПДн
1.10.	Угроза преднамеренного добавления (фальсификации) ПДн
1.11.	Угроза неумышленного (случайного) уничтожения доступных ПДн (записей, файлов, форматирование диска)
1.12.	Угроза преднамеренного уничтожения доступных ПДн (записей, файлов, форматирование диска)
1.13.	Угроза использования для входа в систему чужих идентификаторов и паролей
1.14.	Угроза изменения настроек и режимов работы программного обеспечения (далее - ПО), модификация ПО (удаление, искажение или подмена программных компонентов ИСПДн или средств защиты информации (далее - СЗИ))
1.15.	Угроза нарушения конфиденциальности информации посредством ее утечки по каналам передачи данных
1.16.	Угроза нарушения конфиденциальности информации путем ее непосредственного сбора нарушителем в процессе эксплуатации ИСПДн
1.17.	Угроза подключения к ИСПДн стороннего оборудования (планшетов, смартфонов, фото- и видеокамер, модемов, адаптеров, сетевых карт, считывателей и пр.), внешних накопителей информации (жестких дисков, флеш-дисков, карт памяти и пр.), иных устройств хранения и/или передачи информации, в том числе использующих беспроводные технологии передачи информации, посредством как внешних, так и внутренних разъемов и портов (USB, e-SATA, HDMI, PCI, LPT, COM и др.), имеющихся на средствах вычислительной техники ИСПДн

1.18.	Угроза несанкционированного изменения конфигурационных файлов ПО (настроек экрана, сети, прикладных программ)
1.19.	Угроза установки программных "шпионов"
1.20.	Угроза использования оборудования, оставленного без присмотра, незаблокированных рабочих станций, использования чужих имен и паролей
1.21.	Угроза применения специально созданных программ для повышения прав и привилегий
1.22.	Угроза использования нетрадиционных каналов (например, стеганографии) для передачи ПДн
1.23.	Угроза внедрения программных закладок, формирующих недекларированные возможности программного обеспечения
1.24.	Угроза преднамеренной установки вредоносных программ
1.25.	Ошибки при разработке, развертывании и обслуживании программного обеспечения ИСПДн (в том числе СЗИ)
1.26.	Преднамеренное внесение в программы при их разработке и развертывании вредоносных кодов (программных закладок)
1.27.	Копирование информации с носителей ПДн
1.28.	Хищение, утрата резервных копий носителей ПДн
1.29.	Нарушение порядка резервного копирования ПДн
1.30.	Угроза передачи ПДн по открытым сетям связи за пределы контролируемой зоны
1.31.	Угроза использования программ-анализаторов, пакетов (снифферов) для перехвата ПДн, в т.ч. для перехвата идентификаторов и паролей удаленного доступа
1.32.	Угроза пассивного сбора информации об объектах сети

1.33.	Угроза частичного или полного исчерпания ресурсов
1.34.	Угроза использования ошибок в программном обеспечении
1.35.	Угроза активизации распространяемых злоумышленниками файлов при случайном обращении к ним пользователя
1.36.	Угроза использования возможностей удаленного управления системой
1.37.	Угроза нарушения работоспособности технических средств
1.38.	Утеря или кража оборудования ИСПДн (в том числе резервных носителей информации)
1.39.	Доступ к информации ИСПДн вследствие списания (утилизации) ее носителей, содержащих ПДн
2.	Актуальные угрозы, определяемые согласно требованиям Федеральной службы безопасности Российской Федерации
2.1.	Непредумышленное искажение или удаление программных компонентов ИСПДн
2.2.	Внедрение и использование неучтенных программ
2.3.	Игнорирование организационных ограничений (установленных правил) при работе с ресурсами ИСПДн, включая средства защиты информации
2.4.	Нарушение правил хранения информации ограниченного доступа, используемой при эксплуатации средств защиты информации (в частности: ключевой, парольной и аутентифицирующей информации)
2.5.	Предоставление посторонним лицам возможности доступа к средствам защиты информации, а также к техническим и программным средствам, способным повлиять на выполнение предъявляемых к средствам защиты информации требований
2.6.	Несообщение о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа

2.7.	Внесение негативных функциональных возможностей в технические и программные компоненты криптосредства и среды функционирования (далее - СФ), в том числе с использованием вредоносных программ (компьютерные вирусы и т.д.)
2.8.	Проведение атаки при нахождении в пределах контролируемой зоны
2.9.	Проведение атак на этапе эксплуатации средств криптографической защиты информации (далее - СКЗИ) на следующие объекты: документация на СКЗИ; помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее - СВТ), на которых реализованы СКЗИ
2.10.	Получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: сведения о физических мерах защиты объектов, в которых размещены ресурсы информационной системы; сведения о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы; сведения о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ
2.11.	Использование штатных средств ИСПДн, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий
2.12.	Физический доступ к СВТ, на которых реализованы СКЗИ
2.13.	Возможность воздействовать на аппаратные компоненты СКЗИ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий