

Утверждаю
Директор МБОУ СОШ пгт Краскино
**/И.С. Пантюхова/**
2025



Положение
о защите, хранении, обработке и передаче персональных данных работников
Муниципального бюджетного общеобразовательного учреждения «Средняя
общеобразовательная школа пгт Краскино Хасанского муниципального округа»
(МБОУ СОШ пгт Краскино)

1. Общие положения

1.1. Настоящее Положение МБОУ СОШ пгт Краскино (далее – Учреждение) разработано в соответствии со следующими нормативными правовыми актами:

- Федеральный закон от 27 июля 2006 г. № 152-ФЗ "О персональных данных";
- Федеральным законом от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и защите информации";
- Федеральный закон от 29.12.2012г. № 273-ФЗ «Об образовании в Российской Федерации»
- Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
- Трудовой кодекс Российской Федерации;
- другими действующими нормативными правовыми актами Российской Федерации.

1.2. Персональные данные Работника – информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного Работника.

1.3. К персональным данным Работника относятся:

- фамилия, имя, отчество;
- дата рождения;
- гражданство;
- номер страхового свидетельства;
- ИНН;
- данные об образовании (реквизиты дипломов/иных документов);
- данные о приобретенных специальностях;
- семейное положение;
- данные о членах семьи (степень родства, Ф. И. О., год рождения, паспортные данные, включая прописку и место рождения);
- фактическое место проживания;
- контактная информация;
- данные о военной обязанности;
- данные о текущей трудовой деятельности (дата начала трудовой деятельности, кадровые перемещения, оклады и их изменения, сведения о поощрениях, данные о повышении квалификации и т. п.).

1.4. Обработка персональных данных – сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение персональных данных работников МБОУ СОШ пгт Краскино.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие

обработку персональных данных.

1.5. Персональные данные Работника являются конфиденциальной информацией и не могут быть использованы Работодателем или любым иным лицом в личных целях.

2. Сбор, обработка и защита персональных данных работника

2.1. Все персональные сведения о Работнике Работодатель может получить только от него самого.

В случаях, когда Работодатель может получить необходимые персональные данные Работника только у третьего лица, Работодатель должен уведомить об этом Работника и получить от него письменное согласие.

2.2. Работодатель обязан сообщить Работнику о целях, способах и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа Работника дать письменное согласие на их получение.

2.3. Работодатель не имеет права получать и обрабатывать персональные данные Работника о его политических, религиозных и иных убеждениях, а также о его членстве в общественных объединениях или профсоюзной деятельности, за исключением случаев, предусмотренных законодательством РФ.

2.4. Обработка персональных данных Работника осуществляется исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия Работнику в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности Работника, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

2.5. Обработка указанных персональных данных работников работодателем возможна только с их письменного согласия.

2.6. Письменное согласие работника на обработку своих персональных данных должно включать:

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

- наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;

- цель обработки персональных данных;

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

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

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

2.7. Согласие Работника не требуется, если:

- обработка персональных данных осуществляется на основании Трудового кодекса РФ или иного федерального закона;

- обработка персональных данных осуществляется в целях исполнения трудового договора;

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

- персональные данные являются общедоступными;

- персональные данные относятся к состоянию здоровья Работника 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 работника невозможно;

- персональные данные обрабатываются по требованию полномочных государственных органов в случаях, предусмотренных федеральным законом.

3. Передача и хранение персональных данных работника

3.1. При передаче персональных данных Работника Работодатель должен соблюдать следующие требования:

- не сообщать персональные данные Работника третьей стороне без письменного согласия Работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом;
- не сообщать персональные данные Работника в коммерческих целях без его письменного согласия;
- обработка персональных данных Работника 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;
- предупредить лиц, получивших персональные данные Работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено;
- лица, получившие персональные данные Работника, обязаны соблюдать режим секретности (конфиденциальности);
- осуществлять передачу персональных данных работников в пределах МБОУ СОШ пгт Краскино в соответствии с настоящим Положением;
- разрешать доступ к персональным данным Работника только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретной функции;
- не запрашивать информацию о состоянии здоровья Работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;
- передавать персональные данные Работника представителям работников в порядке, установленном Трудовым кодексом РФ, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

3.2. Персональные данные Работника хранятся в школе, в сейфе на бумажных носителях и на электронных носителях с ограниченным доступом.

3.3. Право доступа к персональным данным Работника имеют:

- директор школы;
- заместитель директора по УВР (информация об образовании и повышении квалификации);
- сотрудники бухгалтерии;
- секретарь (информация о фактическом месте проживания и контактные телефоны работников);
- сотрудники управления образования (доступ к персональным данным работников в ходе плановых проверок);

4. Обязанности работодателя по защите персональных данных работника

4.1. Работодатель обязан за свой счет обеспечить защиту персональных данных Работника от неправомерного их использования или утраты в порядке, установленном законодательством РФ.

4.2. Работодатель обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных федеральными законами в области защиты персональных данных и иными нормативными правовыми актами:

- назначать сотрудника, ответственного за организацию обработки персональных данных;
- издавать документы, определяющие политику МБОУ СОШ пгт Краскино в отношении обработки персональных данных, локальные акты по вопросам обработки и защиты персональных данных;
- применять правовые, организационные и технические меры по обеспечению

безопасности персональных данных;

- при сборе персональных данных Работника-гражданина РФ обеспечивать запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных Работника с использованием баз данных, находящихся на территории РФ в системе Сетевой город образования

- осуществлять внутренний контроль и (или) аудит соответствия обработки персональных данных федеральным законам в области защиты персональных данных и иным нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

- оценивать вред, который может быть причинен субъектам персональных данных в случае нарушения законодательства в области защиты персональных данных, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных законом;

- знакомить работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства в области защиты персональных данных, в том числе с документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучать указанных работников.

4.3. Работодатель обязан ознакомить Работника и его представителей с настоящим Положением и их правами в области защиты персональных данных под роспись.

4.9. Работодатель обязан обеспечить Работнику свободный бесплатный доступ к его персональным данным, включая право на получение копий любой записи, содержащей его персональные данные, за исключением случаев, предусмотренных законом.

4.10. Работодатель обязан по требованию Работника предоставить ему полную информацию о его персональных данных и обработке этих данных.

4.11. Работодатель обязан ежегодно под роспись знакомить Работника с записями в личной карточке Т-2.

5. Права работника на защиту его персональных данных

5.1. Работник в целях обеспечения защиты своих персональных данных, хранящихся у Работодателя, имеет право получать от Работодателя:

- сведения о 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 субъекта персональных данных может повлечь за собой обработка его персональных данных.

5.2 Работник вправе получать доступ к своим персональным данным и знакомиться с ними, а также получать копии любой записи, содержащей персональные данные Работника;

5.3. Работник может требовать от Работодателя уточнить, исключить или исправить неполные, неверные, устаревшие, недостоверные, незаконно полученные или не являющиеся необходимыми для Работодателя персональные данные;

5.4 Работник вправе требовать от Работодателя извещения всех лиц, которым ранее были сообщены неверные или неполные персональные данные Работника, обо всех произведенных в них исключениях, исправлениях или дополнениях.

5.5. Если Работник считает, что Работодатель осуществляет обработку его персональных данных с нарушением требований Федерального закона или иным образом нарушает его права и свободы, Работник вправе обжаловать действия или бездействие Работодателя в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

6. Состав и содержание мер по обеспечению безопасности персональных данных

6.1. В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности персональных данных;
- обеспечение целостности информационной системы и персональных данных;
- обеспечение доступности персональных данных;
- защита среды виртуализации;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;
- управление конфигурацией информационной системы и системы защиты персональных данных.

Состав и содержание мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных, приведены в приложении к Приказу ФСТЭК России от 18.02.2013 года № 21.

6.2. Идентификация и аутентификация субъектов доступа и объектов доступа обеспечивается присвоением субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

6.3. Управление доступом субъектов доступа к объектам доступа обеспечивается управлением правами и привилегиями субъектов доступа, разграничением доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль за соблюдением этих правил.

6.4. Ограничение программной среды обеспечивается установкой и (или) запуском только разрешенного к использованию в информационной системе программного обеспечения и исключает возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

6.5. Машинные носители персональных данных (средств обработки (хранения) персональных данных, съемных машинных носителей персональных данных) исключают возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированное использование съемных машинных носителей персональных данных.

6.6. Регистрация событий безопасности обеспечивают сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

6.7. Антивирусная защита должна обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной

информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

6.8. Обнаружение (предотвращение) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) персональные данные в целях добывания, уничтожения, искажения и блокирования доступа к персональным данным, а также реагирование на эти действия.

6.9. Контроль (анализ) защищенности персональных данных должны обеспечивать контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных.

6.10. Обеспечение целостности информационной системы и персональных данных должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней персональных данных, а также возможность восстановления информационной системы и содержащихся в ней персональных данных.

6.11. Обеспечение доступности персональных данных должны обеспечивать авторизованный доступ пользователей, имеющих права по доступу, к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы.

6.12. Защита среды виртуализации должны исключать несанкционированный доступ к персональным данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействие на них, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

6.13. Защита технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту персональных данных, представленных в виде информативных электрических сигналов и физических полей.

6.14. Защита информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных.

6.15. Выявление инцидентов и реагированию на них должно обеспечивать обнаружение, идентификацию, анализ инцидентов в информационной системе, а также принятие мер по устранению и предупреждению инцидентов.

6.16. Управление конфигурацией информационной системы и системы защиты персональных данных должны обеспечивать управление изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений.

7. Порядок уничтожения, блокирования персональных данных

7.1. В случае выявления неправомерной обработки персональных данных при обращении

Работника Работодатель обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому Работнику, с момента такого обращения.

7.2. В случае выявления неточных персональных данных при обращении Работника Работодатель обязан осуществить блокирование персональных данных, относящихся к этому Работнику, с момента такого обращения, если блокирование персональных данных не нарушает права и законные интересы Работника или третьих лиц.

7.3. В случае подтверждения факта неточности персональных данных Работодатель на основании сведений, представленных Работником, или иных необходимых документов обязан уточнить персональные данные в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

7.4. В случае выявления неправомерной обработки персональных данных, осуществляемой Работодателем, Работодатель в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных.

7.5. Если обеспечить правомерность обработки персональных данных невозможно, Работодатель в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные.

7.6. Об устранении допущенных нарушений или об уничтожении персональных данных Работодатель обязан уведомить Работника.

7.7. В случае достижения цели обработки персональных данных Работодатель обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено трудовым договором.

7.8. В случае отзыва Работником согласия на обработку его персональных данных Работодатель обязан прекратить их обработку и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено трудовым договором.

7.9. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в пунктах 6.4-6.8 настоящего Положения, Работодатель осуществляет блокирование таких персональных данных и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

8. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника

8.1. Работники МБОУ СОШ пгт Краскино, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

8.2. Моральный вред, причиненный Работнику вследствие нарушения его прав, нарушения правил обработки персональных данных, подлежит возмещению в соответствии с законодательством РФ. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных Работником убытков.

9. Заключительные положения

9.1. Настоящее Положение вступает в силу с момента его утверждения директором МБОУ СОШ пгт Краскино и действует бессрочно, до замены его новым Положением.

9.2. Все изменения в Положение вносятся приказом директора МБОУ СОШ пгт Краскино.

9.3. Все работники МБОУ СОШ пгт Краскино должны быть ознакомлены с настоящим Положением под роспись.