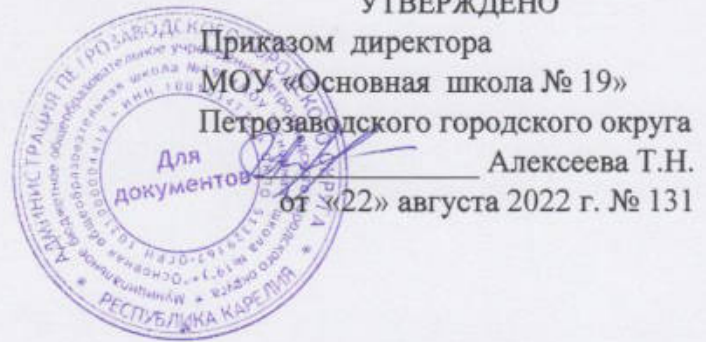


УТВЕРЖДЕНО



## ПОЛИТИКА ЗАЩИТЫ И ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Муниципального бюджетного общеобразовательного учреждения Петрозаводского городского округа «Основная общеобразовательная школа № 19»  
(Далее – МОУ «Основная школа № 19»)

### 1. Общие положения

1.1. Настоящая Политика МОУ «Основная школа № 19» в отношении обработки персональных данных (далее - Политика) разработана во исполнение требований п. 2 ч. 1 ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон о персональных данных), в соответствии с Федеральным законом «Об образовании в Российской Федерации»; постановлением Правительства РФ от 15.09.2008 №687 «Об утверждении перечня персональных данных, обрабатываемых в Министерстве юстиции Российской Федерации в связи с реализацией трудовых отношений; Федеральным законом от 14 июля 2022 г. № 266-ФЗ «О внесении изменений в Федеральный закон о «О персональных данных»; отдельными законодательными актами Российской Федерации, а также типовой формой согласия на обработку персональных данных; Трудовым кодексом Российской Федерации; Гражданским кодексом Российской Федерации; Конституцией Российской Федерации и иными нормативно-правовыми актами в целях обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.2. Политика действует в отношении всех персональных данных, которые обрабатывает МОУ «Основная школа № 19» (далее – Оператор).

1.3. Настоящая Политика вступает в силу с момента ее утверждения директором школы.

1.4. Порядок обработки персональных данных утверждается директором школы. Все работники школы должны быть ознакомлены под роспись с настоящей Политикой, в редакции, действующей на момент ознакомления. Родители (при их отсутствии – законные представители) учащихся школы должны быть ознакомлены с настоящей Политикой под роспись.

1.5. Политика распространяется на отношения в области обработки персональных данных, возникшие у Оператора как до, так и после утверждения настоящей Политики.

1.6. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности снимается в случаях их обезличивания и по истечении 75 лет срока их хранения, или продлевается на основании заключения экспертной комиссии Оператора, если иное не определено законом.

1.7. Во исполнение требований ч. 2 ст. 18.1 Закона о персональных данных настоящая Политика публикуется в свободном доступе в информационно-телекоммуникационной сети Интернет на сайте Оператора.

### 2. Термины и принятые сокращения

**Персональные данные (Далее – ПД)** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

**Персональные данные, разрешенные субъектом персональных данных для распространения** – это персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

**Оператор персональных данных** (оператор) –юридическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

**Субъекты персональных данных:**

- работники – лица, имеющие трудовые отношения с Оператором, либо кандидаты на вакантную должность, вступившие с Оператором в отношения по поводу приема на работу.

- Обучающиеся, воспитанники и их родители (законные представители), передавшие свои персональные данные Оператору на добровольной основе и (или) в рамках выполнения требований нормативно-правовых актов для их обработки.

**Обработка персональных данных** – любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без их использования. Обработка персональных данных включает в себя в том числе:

- сбор;
- запись;
- систематизацию;
- накопление;
- хранение;
- уточнение (обновление, изменение);
- извлечение;
- использование;
- передачу (предоставление, доступ);
- распространение;
- обезличивание;
- блокирование;
- удаление;
- уничтожение.

**Автоматизированная обработка персональных данных** – обработка персональных данных с помощью средств вычислительной техники.

**Предоставление персональных данных** – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

**Блокирование персональных данных** – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

**Уничтожение персональных данных** – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

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

**Информационная система персональных данных** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку, информационных технологий и технических средств.

**Трансграничная передача персональных данных** – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

### **3. Основные права и обязанности Оператора**

3.1. Оператор при сборе персональных данных обязан предоставить субъекту персональных данных по его просьбе информацию, касающуюся обработки его персональных данных.

3.2. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, Оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

3.3. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети интернет, Оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных Федеральном законе «О персональных данных».

3.4. Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

3.5. Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к настоящей Политике, к сведениям о реализуемых требованиях к защите персональных данных. Оператор в случае осуществления сбора персональных данных с использованием информационно-телекоммуникационных сетей обязан опубликовать в соответствующей информационно-телекоммуникационной сети Политику и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием соответствующей информационно-телекоммуникационной сети.

3.6. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

3.7. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора. Лицо, осуществляющее обработку персональных данных по поручению Оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом «О персональных данных». В поручении Оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона «О персональных данных».

3.8. В случае изменения сведений об обработке персональных данных, Оператору необходимо проинформировать Роскомнадзор не позднее 15-го числа месяца, следующего за месяцем, в котором возникли такие изменения.

#### 4. Основные права и обязанности субъекта персональных данных

4.1. Субъект персональных данных вправе получать информацию, касающуюся обработки своих персональных данных:

- обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, предусмотренных требованиями ч.2 ст.10. Федерального закона № 152-ФЗ, если:

- 1) субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;
- 2) обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется с соблюдением запретов и условий, предусмотренных статьей 10.1 настоящего Федерального закона;
- 3) обработка персональных данных необходима в связи с реализацией международных договоров Российской Федерации о реадмиссии;
- 4) обработка персональных данных осуществляется в соответствии с Федеральным законом от 25 января 2002 года N 8-ФЗ "О Всероссийской переписи населения";
- 5) обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, пенсионным законодательством Российской Федерации;
- 6) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно;
- 7) 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;
- 8) обработка персональных данных членов (участников) общественного объединения или религиозной организации осуществляется соответствующими общественным объединением или религиозной организацией, 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;
- 9) обработка персональных данных необходима для установления или осуществления прав субъекта персональных данных или третьих лиц, а равно и в связи с осуществлением правосудия;
- 10) обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, об исполнительном производстве, уголовно-исполнительным законодательством Российской Федерации;
- 11) обработка полученных в установленных законодательством Российской Федерации случаях персональных данных осуществляется органами прокуратуры в связи с осуществлением ими прокурорского надзора;
- 12) обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством;
- 13) обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации, государственными органами, муниципальными органами или организациями в целях устройства детей, оставшихся без попечения родителей, на воспитание в семьи граждан;
- 14) обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о гражданстве Российской Федерации.

Обработка персональных данных, касающихся состояния здоровья, полученных в результате обезличивания персональных данных, допускается в целях повышения эффективности государственного или муниципального управления, а также в иных целях, предусмотренных Федеральным законом от 24 апреля 2020 года N 123-ФЗ "О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации - городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона "О персональных данных" и Федеральным законом от 31 июля 2020 года N 258-ФЗ "Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации", в порядке и на условиях, которые предусмотрены указанными федеральными законами.

4.2. Субъект персональных данных вправе требовать от Оператора:

- уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;
- подтверждение факта обработки ПД Оператором;
- правовые основания и цели обработки ПД;
- цели и применяемые Оператором способы обработки ПД;
- наименование и место нахождения Оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к ПД или которым могут быть раскрыты ПД на основании договора с Оператором или на основании федерального закона;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом ПД прав, предусмотренных настоящим Федеральным законом;
- наименование или фамилия, имя, отчество и адрес лица, осуществляющего обработку ПД по поручению Оператора, если обработка поручена или будет поручена такому лицу;
- обращение к Оператору и направление ему запросов;

4.2. Если субъект персональных данных считает, что Оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона «О персональных данных» или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Оператора в уполномоченном органе по защите прав субъектов персональных данных или в судебном порядке.

4.3. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке

## **5. Порядок и условия обработки персональных данных**

5.1. Оператор обрабатывает персональные данные на основании:

- Трудового кодекса Российской Федерации;
- иных федеральных законов и прочих нормативных правовых актов;
- устава Оператора;
- договоров, заключаемых между Оператором и субъектами персональных данных;
- согласий на обработку персональных данных;

5.1. Обработка персональных данных осуществляется Оператором в соответствии с требованиями законодательства Российской Федерации.

5.2. Обработка персональных данных осуществляется с согласия субъектов персональных данных на обработку их персональных данных, а также без такового в случаях, предусмотренных законодательством Российской Федерации.

5.3. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью.

5.4. Письменное согласие субъекта 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 и адрес Оператора;
- 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;
- способ его отзыва;
- подпись субъекта персональных данных.

5.5. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных.

5.6. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, может быть предоставлено оператору:

- непосредственно;
- с использованием информационной системы уполномоченного органа по защите прав субъектов персональных данных.

5.7. Оператор осуществляет как автоматизированную, так и неавтоматизированную обработку персональных данных.

5.8. Оператор не принимает, не снимает и не хранит копии личных документов субъектов персональных данных.

5.9. Документы, которые субъекты персональных данных предъявляют Оператору для хранения в оригинале (справки, медицинские заключения и т.д.) хранятся в личном деле работника в течение 50 лет после расторжения с работником трудового договора.

5.9.1. После истечения срока нормативного хранения документов, которые содержат ПД работника, документы подлежат уничтожению. Для этого Оператор создает экспертную комиссию и проводит экспертизу ценности документов. В ходе проведения экспертизы комиссия отбирает дела с истекшими сроками хранения и по итогам отбора составляет акт о выделении к уничтожению дел, не подлежащих хранению.

5.10. К обработке персональных данных допускаются работники Оператора, в должностные обязанности которых входит обработка персональных данных.

5.11. Обработка персональных данных осуществляется путем:

- получения персональных данных в устной и письменной форме непосредственно с согласия субъекта персональных данных на обработку или распространение его персональных данных;
- внесения персональных данных в журналы, реестры и информационные системы Оператора;
- использования иных способов обработки персональных данных.

5.12. Не допускается раскрытие третьим лицам и распространение персональных данных без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

5.13. Передача персональных данных органам дознания и следствия, в Федеральную налоговую службу, Пенсионный фонд, Фонд социального страхования и другие уполномоченные органы

исполнительной власти и организации осуществляется в соответствии с требованиями законодательства Российской Федерации.

5.14. Оператор организует обработку персональных данных в следующем порядке:

- 1) назначает ответственного за организацию обработки персональных данных, устанавливает перечень лиц, имеющих доступ к персональным данным;
- 2) издает настоящую Политику, локальные акты по вопросам обработки персональных данных;
- 3) применяет правовые, организационные и технические меры по обеспечению безопасности персональных данных;
- 4) осуществляет внутренний контроль и (или) аудит соответствия обработки персональных данных Федеральному закону «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, настоящей Политике, локальным актам Оператора;
- 5) осуществляет оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных», определяет соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных данным Федеральным законом;
- 6) знакомит работников Оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, настоящей Политики, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

5.15. Оператор при обработке персональных данных принимает необходимые правовые, организационные и технические меры, в том числе:

- 1) определяет угрозы безопасности персональных данных при их обработке в информационных системах персональных данных;
- 2) применяет организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимые для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;
- 3) применяет прошедшие в установленном порядке процедуру оценки соответствия средства защиты информации;
- 4) оценивает эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- 5) учитывает машинные носители персональных данных;
- 6) обнаруживает факты несанкционированного доступа к персональным данным и принимает меры;
- 7) восстанавливает персональные данные, модифицированные или уничтоженные вследствие несанкционированного доступа к ним;
- 8) устанавливает правила доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечивает регистрацию и учет всех действий, совершаемых с персональными данными в информационной системе персональных данных.

5.16. При обработке персональных данных Оператор выполняет, в частности, сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

5.17. В целях обеспечения сохранности и конфиденциальности персональных данных все операции с персональными данными должны выполняться только работниками Оператора, осуществляющими данную работу в соответствии с трудовыми обязанностями.

5.18. Оператор получает персональные данные непосредственно от субъектов персональных данных или их представителей, наделенных соответствующими полномочиями. Согласия субъекта на получение его персональных данных от третьих лиц не требуется в случаях, когда согласие субъекта на передачу его персональных данных третьим лицам получено от него в письменном

виде при заключении договора с Оператором, а также в случаях, установленных федеральным законом.

5.19. Запрещается хранение документов с персональными данными и их копий на рабочих местах и (или) в открытом доступе, оставлять шкафы (сейфы) открытыми в случае выхода работника из рабочего помещения.

5.20. В электронном виде документы, содержащие персональные данные, разрешается хранить в специализированных базах данных или в специально отведенных для этого директориях с ограничением и разграничением доступа. Копирование таких данных запрещено.

5.21. При увольнении работника, имеющего доступ к персональным данным, прекращении доступа к персональным данным, документы и иные носители, содержащие персональные данные, сдаются работником своему непосредственному руководителю.

## **6. Порядок обработки персональных данных в информационных системах**

6.1. Обработка персональных данных в информационных системах осуществляется после реализации организационных и технических мер по обеспечению безопасности персональных данных, определенных с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

6.2. Обеспечение безопасности при обработке персональных данных, содержащихся в информационных системах органов и подведомственных организаций, осуществляется в соответствии с постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом ФСТЭК России от 18.02.2013 № 21.

6.3. Уполномоченному работнику, имеющему право осуществлять обработку персональных данных в информационных системах, предоставляется уникальный логин и пароль для доступа к соответствующей информационной системе. Доступ предоставляется в соответствии с функциями, предусмотренными должностными обязанностями работника.

6.4. Информация может вноситься как в автоматическом режиме при получении персональных данных с официального сайта в сети интернет, так и в ручном режиме при получении информации на бумажном носителе или в ином виде, не позволяющем осуществлять ее автоматическую регистрацию.

6.5. Обеспечение безопасности персональных данных, обрабатываемых в информационных системах органов, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным.

6.6. В случае выявления нарушений порядка обработки персональных данных уполномоченными работниками незамедлительно принимаются меры по установлению причин нарушений и их устранению.

6.7. 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;
- 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 и 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, и реагирование на них;
- управление конфигурацией информационной системы и системы защиты персональных данных.

6.8. Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия. Угрозы первого типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе. Угрозы второго типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы третьего типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Федерального закона «О персональных данных».

6.9. В соответствии с пунктом 11 статьи 19 Федерального закона «О персональных данных» под уровнем защищенности персональных данных понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

При обработке персональных данных в информационных системах устанавливаются четыре уровня защищенности персональных данных.

6.9.1. Необходимость обеспечения первого уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

- а) для информационной системы актуальны угрозы первого типа и информационная система обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных;
- б) для информационной системы актуальны угрозы второго типа и информационная система обрабатывает специальные категории персональных данных более чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора.

6.9.2. Необходимость обеспечения второго уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

- а) для информационной системы актуальны угрозы первого типа и информационная система обрабатывает общедоступные персональные данные;
- б) для информационной системы актуальны угрозы второго типа и информационная система обрабатывает специальные категории персональных данных сотрудников Оператора или специальные категории персональных данных менее чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора;
- в) для информационной системы актуальны угрозы второго типа и информационная система обрабатывает биометрические персональные данные;

г) для информационной системы актуальны угрозы второго типа и информационная система обрабатывает общедоступные персональные данные более чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора;

д) для информационной системы актуальны угрозы второго типа и информационная система обрабатывает иные категории персональных данных более чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора;

е) для информационной системы актуальны угрозы третьего типа и информационная система обрабатывает специальные категории персональных данных более чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора.

6.9.3. Необходимость обеспечения третьего уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы второго типа и информационная система обрабатывает общедоступные персональные данные сотрудников Оператора или общедоступные персональные данные менее чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора;

б) для информационной системы актуальны угрозы второго типа и информационная система обрабатывает иные категории персональных данных сотрудников Оператора или иные категории персональных данных менее чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора;

в) для информационной системы актуальны угрозы третьего типа и информационная система обрабатывает специальные категории персональных данных сотрудников Оператора или специальные категории персональных данных менее чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора;

г) для информационной системы актуальны угрозы третьего типа и информационная система обрабатывает биометрические персональные данные;

д) для информационной системы актуальны угрозы третьего типа и информационная система обрабатывает иные категории персональных данных более чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора.

6.9.4. Необходимость обеспечения четвертого уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы третьего типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы третьего типа и информационная система обрабатывает иные категории персональных данных сотрудников Оператора или иные категории персональных данных менее чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора.

6.10. Состав и содержание мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных, приведены в приложении к Составу и содержанию организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом ФСТЭК России от 18.02.2013 № 21.

## **7. Цели обработки персональных данных:**

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

7.2. Обработка Оператором персональных данных осуществляется в следующих целях:

- обеспечение соблюдения Конституции, федеральных законов и иных нормативных правовых актов Российской Федерации;
- осуществление своей деятельности в соответствии с уставом Оператора;

- ведение кадрового делопроизводства;
- содействие работникам в трудоустройстве, получении образования и продвижении по службе, обеспечение личной безопасности работников, контроль количества и качества выполняемой работы, обеспечение сохранности имущества;
- привлечение и отбор кандидатов на работу у Оператора;
- организация постановки на индивидуальный (персонифицированный) учет работников в системе обязательного пенсионного страхования;
- заполнение и передача в органы исполнительной власти и иные уполномоченные организации требуемых форм отчетности;
- осуществление гражданско-правовых отношений;
- ведение бухгалтерского учета;
- осуществление пропускного режима.

7.3. Обработка персональных данных работников может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов.

7.4. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

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

7.6. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

7.7. Категории субъектов персональных данных.

Обрабатываются ПД следующих субъектов ПД:

7.7.1. Физические лица, состоящие с МОУ «Основная школа № 19» в трудовых отношениях; физические лица, уволившиеся из МОУ «Основная школа № 19»; физические лица, являющиеся кандидатами на работу;

7.7.2. Физические лица, принимающиеся на обучение и воспитание в МОУ «Основная школа № 19».

7.7.3. Родители или законные представители воспитанников и обучающихся.

7.8. В отношении категорий, указанных в пункте 7.7.1. (за исключением членов семьи работников), обрабатываются:

- фамилия, имя, отчество;
- дата и место рождения;
- адреса места жительства и регистрации;
- контактный телефон;
- гражданство;
- образование;
- профессия, должность;
- стаж работы;
- семейное положение, наличие детей;
- серия и номер основного документа, удостоверяющего личность, сведения о выдаче указанного документа и выдавшем его органе;
- данные страхового свидетельства государственного пенсионного страхования;
- идентификационный номер налогоплательщика;
- табельный номер;
- сведения о доходах;

- сведения о воинском учете;
- сведения о судимостях;
- сведения о повышении квалификации, о профессиональной переподготовке;
- сведения о наградах (поощрениях), почетных званиях;
- сведения о социальных гарантиях;
- сведения о состоянии здоровья, влияющие на выполнение трудовой функции;

7.9. В отношении категорий, указанных в пункте 7.7.2. обрабатываются:

- фамилия, имя, отчество;
- дата и место рождения;
- адреса места жительства и регистрации;
- гражданство;
- серия и номер основного документа, удостоверяющего личность, сведения о выдаче указанного документа и выдавшем его органе;
- данные страхового свидетельства государственного пенсионного страхования;
- сведения о состоянии здоровья;
- сведения о социальных гарантиях;

7.10. В отношении категорий, указанных в пункте 7.7.3. обрабатываются:

- фамилия, имя, отчество;
- дата и место рождения;
- адреса места жительства и регистрации;
- контактный телефон;
- гражданство;
- семейное положение, наличие детей;
- серия и номер основного документа, удостоверяющего личность, сведения о выдаче указанного документа и выдавшем его органе;
- данные страхового свидетельства государственного пенсионного страхования;
- сведения о социальных гарантиях;

7.11. ПД, обрабатываемые Оператором:

- данные, полученные при осуществлении трудовых отношений;
- данные, полученные для осуществления отбора кандидатов на работу;
- данные, полученные при зачислении, обучении и воспитании обучающихся и воспитанников у Оператора;

## **8. Хранение персональных данных.**

8.1. ПД субъектов могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде.

8.2. ПД, зафиксированные на бумажных носителях, хранятся в запираемых шкафах либо в запираемых помещениях с ограниченным правом доступа.

8.3. ПД субъектов, обрабатываемые с использованием средств автоматизации в разных целях, хранятся в разных папках.

8.4. Не допускается хранение и размещение документов, содержащих ПД, в открытых электронных каталогах (файлообменниках) в ИСПД.

8.5. Хранение ПД в форме, позволяющей определить субъекта ПД, осуществляется не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

## **9. Защита персональных данных**

9.1. В соответствии с требованиями нормативных документов Оператором создана система защиты персональных данных (СЗПД), состоящая из подсистем правовой, организационной и технической защиты.

9.2. Подсистема правовой защиты представляет собой комплекс правовых, организационно-распорядительных и нормативных документов, обеспечивающих создание, функционирование и совершенствование СЗПД.

9.3. Подсистема организационной защиты включает в себя организацию структуры управления СЗПД, разрешительной системы, защиты информации при работе с сотрудниками, партнерами и сторонними лицами.

9.4. Подсистема технической защиты включает в себя комплекс технических, программных, программно-аппаратных средств, обеспечивающих защиту ПД.

9.5. Основными мерами защиты ПД, используемыми Оператором, являются:

9.5.1. Назначение лица, ответственного за обработку ПД, которое осуществляет организацию обработки ПД, обучение и инструктаж, внутренний контроль за соблюдением учреждением и его работниками требований к защите ПД.

9.5.2. Определение актуальных угроз безопасности ПД при их обработке в ИСПД и разработка мер и мероприятий по защите ПД.

9.5.3. Разработка политики в отношении обработки персональных данных.

9.5.4. Установление правил доступа к ПД, обрабатываемых в ИСПД, а также обеспечение регистрации и учета всех действий, совершаемых с ПД в ИСПД.

9.5.5. Установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их производственными обязанностями.

9.5.6. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации.

9.5.7. Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами.

9.5.8. Соблюдение условий, обеспечивающих сохранность ПД и исключающих несанкционированный к ним доступ.

9.5.9. Обнаружение фактов несанкционированного доступа к персональным данным и принятие мер.

9.5.10. Восстановление ПД, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

9.5.11. Обучение работников Оператора, непосредственно осуществляющих обработку персональных данных, положениям законодательства РФ о персональных данных, в том числе требованиям к защите персональных данных, документам, определяющим политику Оператора в отношении обработки персональных данных, локальным актам по вопросам обработки персональных данных.

9.5.12. Осуществление внутреннего контроля и аудита.

## **10. Актуализация, исправление, удаление и уничтожение персональных данных, ответы на запросы субъектов на доступ к персональным данным**

10.1. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- 1) подтверждение факта обработки персональных данных оператором;
- 2) правовые основания и цели обработки персональных данных;
- 3) цели и применяемые оператором способы обработки персональных данных;
- 4) наименование и место нахождения Оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Оператором или на основании федерального закона;

- 5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- 6) сроки обработки персональных данных, в том числе сроки их хранения;
- 7) порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»;
- 8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- 9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка поручена или будет поручена такому лицу;
- 10) иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами.

10.2. Указанные выше сведения должны быть предоставлены субъекту персональных данных Оператором в доступной форме и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

10.3. Сведения, указанные в пункте 10.1, предоставляются субъекту персональных данных или его представителю Оператором при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с Оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

10.4. В случае если сведения, указанные в пункте 10.1, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к Оператору или направить ему повторный запрос в целях получения сведений, указанных в пункте 10.1, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

10.5. Субъект персональных данных вправе обратиться повторно к Оператору или направить ему повторный запрос в целях получения сведений, указанных в пункте 10.1, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в пункте 10.4, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в пункте 10.1, должен содержать обоснование направления повторного запроса.

10.6. Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 10.4 и 10.5. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Операторе.

10.7. Оператор обязан сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя в течение 10

рабочих дней с даты получения запроса субъекта персональных данных или его представителя. Указанный срок может быть продлен, но не более чем на 5 рабочих дней в случае направления в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

10.8. Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных.

10.9. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, Оператор обязан внести в них необходимые изменения.

10.10. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Оператор обязан уничтожить такие персональные данные.

10.11. Оператор обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

10.12. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя, либо по запросу субъекта персональных данных или его представителя, либо уполномоченного органа по защите прав субъектов персональных данных Оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) с момента такого обращения или получения указанного запроса на период проверки.

10.13. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных Оператор обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

10.14. В случае подтверждения факта неточности персональных данных Оператор на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

10.15. В случае выявления неправомерной обработки персональных данных, осуществляемой Оператором или лицом, действующим по поручению Оператора, Оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению Оператора. В случае если обеспечить правомерность обработки персональных данных невозможно, Оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение.

Об устранении допущенных нарушений или об уничтожении персональных данных Оператор обязан уведомить субъекта персональных данных или его представителя в течение десяти дней, а в случае, если обращение субъекта персональных данных или его представителя либо запрос

уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

10.16. В случае достижения цели обработки персональных данных Оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) в срок, не превышающий десяти дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Оператором и субъектом персональных данных либо если Оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

10.17. Уведомлять Роскомнадзор об изменениях персональных данных в базе Оператора в течение пятнадцати дней;

10.18. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора), если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Оператором и субъектом персональных данных либо если Оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

10.19. Уничтожение документов (носителей), содержащих ПД, производится путем сожжения, дробления (измельчения), химического разложения, превращения в бесформенную массу или порошок. Для уничтожения бумажных документов допускается применение шредера.

10.20. ПД на электронных носителях уничтожаются путем стирания или форматирования носителя.

10.21. Факт уничтожения ПД подтверждается документально актом об уничтожении носителей.

10.22. В случае отсутствия возможности уничтожения персональных данных в течение указанных сроков Оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

## **11. Доступ к персональным данным.**

11.1. Приказом директора МОУ «Основная школа № 19» назначается сотрудник, ответственный за организацию обработки ПД.

11.2. Лица, допущенные к обработке ПД, в обязательном порядке под роспись знакомятся с настоящей Политикой и подписывают обязательство о неразглашении информации, содержащей ПД.

11.3. Право внутреннего доступа к ПД обучающихся и воспитанников МОУ «Основная школа № 19», их родителей (законных представителей) имеют:

- директор МОУ «Основная школа № 19»;
- родители обучающегося или воспитанника;



- работники бухгалтерии (к данным, которые необходимы для выполнения функций по приему платы за организацию питания )

- классный руководитель;

11.4. Внешний доступ к ПД осуществляется при соблюдении требований Закона № 152-ФЗ.

11.5. В случае, если лицо, обратившееся с запросом, не обладает соответствующими полномочиями на получение ПД, либо отсутствует письменное согласие субъекта на передачу его ПД, Оператор вправе отказать в предоставлении ПД. В этом случае лицу, обратившемуся с запросом, направляется письменный мотивированный отказ в предоставлении запрашиваемой информации.

## **12. Заключительные положения**

12.1. Политика является общедоступным документом.

12.2. Ответственность лиц, имеющих доступ к персональным данным, определяется действующим законодательством Российской Федерации.