

Департамент образования и молодежной политики Нефтеюганского  
района

Нефтеюганское районное муниципальное общеобразовательное  
бюджетное учреждение «Пойковская средняя общеобразовательная школа № 2»

**ПРИКАЗ**

02.08.2017

№ 387-О

**О защите информации**

В соответствии с требованиями Федерального закона Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»:

1. Возложить обязанности по защите информации:

1.1. Назначить ответственным за организацию обработки персональных данных Директора Нефтеюганского районного муниципального общеобразовательного бюджетного учреждения «Пойковская средняя общеобразовательная школа №2» (далее – Пойковская СОШ №2) Морозову Елену Николаевну.

1.2. Назначить ответственным за обеспечение безопасности персональных данных в информационной системе персональных данных (администратором информационной безопасности ИСПДн) «РИС ГИА НРМОБУ «ПСОШ №2» заместителя директора по информационной безопасности Мельник Елену Юрьевну.

1.3. Назначить ответственным за эксплуатацию ИСПДн «РИС ГИА НРМОБУ «ПСОШ №2» техника Стороженко Дмитрия Александровича.

1.4. Утвердить перечень лиц, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей и Перечень лиц, допущенных в помещения, в которых располагаются технические средства ИСПДн, согласно приложению 1 к настоящему распоряжению.

1.5. Утвердить перечень должностей, ответственных за проведение мероприятий по обезличиванию обрабатываемых ПДн и Перечень должностей, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным согласно приложению 2 к настоящему распоряжению.

2. Создать комиссию по защите информации:

2.1. Утвердить состав комиссии по защите информации согласно приложению 3 к настоящему распоряжению.

2.2. Утвердить положение о комиссии по защите информации согласно

приложению 4 к настоящему распоряжению.

3. Утвердить типовые формы документов по защите информации:

3.1. Обязательство о неразглашении информации, содержащей персональные данные, типовую форму согласия субъекта на обработку их персональных данных и типовую форму разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные, согласно приложению 5 к настоящему распоряжению.

3.2. Журналы по защите информации согласно приложению 6 к настоящему распоряжению.

3.3. Акт определения уровня защищенности ПДн и класса защищенности ГИС согласно приложению 7 к настоящему распоряжению.

3.4. Акт об уничтожении персональных данных субъектов персональных данных согласно приложению 8 к настоящему распоряжению.

4. Утвердить перечень информационных систем персональных данных согласно приложению 9 к настоящему распоряжению.

5. Утвердить перечень обрабатываемых персональных данных согласно приложению 10 к настоящему распоряжению.

6. Утвердить положение об организации режима обеспечения безопасности помещений, в которых размещены информационные системы персональных данных, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения согласно приложению 11 к настоящему распоряжению.

7. Утвердить политику в отношении обработки персональных данных согласно приложению 12.

8. Утвердить инструкции и правила по защите информации:

– Инструкцию ответственного за организацию обработки персональных данных согласно приложению 13 к настоящему распоряжению;

– Инструкцию ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных согласно приложению 14 к настоящему распоряжению;

– Инструкцию ответственного за эксплуатацию информационных систем персональных данных согласно приложению 15 к настоящему распоряжению;

– Правила работы лиц, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей, согласно приложению 16 к настоящему распоряжению;

– Правила рассмотрения запросов субъектов персональных данных согласно приложению 17 к настоящему распоряжению;

– Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, согласно приложению 18 к настоящему распоряжению;

– Порядок уничтожения персональных данных при достижении целей обработки и (или) при наступлении законных оснований согласно приложению 19 к настоящему распоряжению;

– Правила работы с обезличенными данными в случае обезличивания ПДн

приложению 20 к настоящему распоряжению;

– Инструкцию по организации резервного копирования согласно приложению 21 к настоящему распоряжению;

– Инструкцию по организации парольной защиты согласно приложению 22 к настоящему распоряжению;

– Инструкцию по организации антивирусной защиты согласно приложению 23 к настоящему распоряжению;

– Инструкцию о пропускном и внутриобъектовом режимах согласно приложению 24 к настоящему распоряжению;

– Инструкцию по работе с инцидентами информационной безопасности согласно приложению 25 к настоящему распоряжению;

9. Утвердить план мероприятий по защите информации согласно приложению 26 к настоящему распоряжению.

Директор Пойковской СОШ №2

Морозова Е.Н.

## **ПОЛИТИКА в отношении обработки персональных данных**

### **1. Общие положения**

1.1. Политика в отношении обработки персональных данных в Пойковской СОШ №2 (далее – Политика) разработана в соответствии с Конституцией Российской Федерации, Федеральным законом Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», Трудовым кодексом Российской Федерации.

1.2. Политика определяет порядок и условия обработки персональных данных в Пойковской СОШ №2 (далее – Оператор) с использованием средств автоматизации и без использования таких средств.

1.3. Обработка персональных данных осуществляется в целях предоставления государственных и муниципальных услуг в соответствии с административными регламентами предоставления указанных услуг на основании соглашений, заключенных федеральными органами исполнительной власти и органами государственных внебюджетных фондов с Оператором, обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получении образования и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

### **2. Основные понятия, используемые в настоящей Политике**

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

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

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

2.4. Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

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

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

2.7. 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.

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

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

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

### 3. Принципы обработки персональных данных

3.1. Обработка персональных данных осуществляется на законной основе.

3.2. Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

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

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

3.5. Содержание и объем персональных данных соответствуют заявленным целям обработки. Обрабатываемые персональные данные не являются избыточным по отношению к заявленным целям обработки.

3.6. При обработке персональных данных обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператором обеспечивается принятие необходимых мер по удалению или уточнению неполных или неточных данных.

3.7. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

### 4. Условия обработки персональных данных

4.1. Обработка персональных данных осуществляется с соблюдением принципов и правил, предусмотренных Федеральным законом «О персональных данных». Обработка персональных данных допускается в следующих случаях:

4.1.1. Обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

4.1.2. Обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом для осуществления и выполнения возложенных законодательством Российской Федерации на Оператора функций, полномочий и обязанностей;

4.1.3. Обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», включая регистрацию

субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг;

4.1.4. Обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

4.1.5. Обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

4.1.6. Обработка персональных данных необходима для осуществления прав и законных интересов Оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

4.1.7. Осуществляется обработка персональных данных, доступ неограниченного круга лиц, к которым предоставлен субъектом персональных данных либо по его просьбе;

4.1.8. Осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

4.2. В случае если Оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет Оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

## 5. Конфиденциальность персональных данных

5.1. Оператор и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

## 6. Право субъекта персональных данных на доступ к его персональным данным.

6.1. Субъект персональных данных имеет право на получение сведений, указанных в п. 6.7 настоящей Политики, за исключением случаев, при которых доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц. 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.

6.2. Сведения, указанные в п. 6.7 настоящей Политики, 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.

6.3. Сведения, указанные в п. 6.7 настоящей Политики, 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 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.

6.4. В случае если сведения, указанные в п. 6.7 настоящей Политики, 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 п. 6.7 настоящего положения, 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.

6.5. Субъект персональных данных вправе обратиться повторно к Оператору или направить ему запрос в целях получения сведений, указанных в п. 6.7 настоящей Политики, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в п. 6.4 настоящей Политики, 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 п. 6.3 настоящей Политики, должен содержать основание направления повторного запроса.

6.6. Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса, несоответствующего условиям, предусмотренным п. 6.3 и п. 6.4. настоящей Политики. Такой отказ должен быть мотивированным. Обязанность предоставления доказательств обоснованности отказа в выполнении повторного запроса лежит на Операторе.

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

6.7.1. Подтверждение факта обработки персональных данных Оператором;

6.7.2. Правовые основания и цели обработки персональных данных;

6.7.3. Цели и применяемые Оператором способы обработки персональных данных;

6.7.4. Наименование и местонахождение Оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к персональным данным или которые могут быть раскрыты персональные данные на основании договора с Оператором или на основании федерального закона;

6.7.5. Обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок предоставления таких данных не предусмотрен федеральным законом;

6.7.6. Сроки обработки персональных данных, в том числе сроки их хранения;

6.7.7. Порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»;

6.7.8. Информацию об осуществленной или о предполагаемой трансграничной передаче данных;

6.7.9. Наименование или имя, фамилию, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка поручена или будет поручена такому лицу.

6.7.10. Иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами.

## 7. Право на обжалование действий или бездействий Оператора

7.1. 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 бездействия Оператора в

уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

7.2. 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.

## 8. Обязанности Оператора при сборе персональных данных

8.1. При сборе персональных данных Оператор обязан предоставить субъекту персональных данных по его просьбе информацию, предусмотренную частью 6.7 настоящей Политики.

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

8.3. Если персональные данные получены не от субъекта персональных данных, Оператор, за исключением случаев, предусмотренных п. 8.4 настоящей Политики, до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:

8.3.1. Наименование либо фамилия, имя, отчество и адрес Оператора или его представителя;

8.3.2. Цель обработки персональных данных и ее правовое основание;

8.3.3. Предполагаемые пользователи персональных данных;

8.3.4. Установленные настоящим Федеральным законом права субъекта персональных данных;

8.3.5. Источник получения персональных данных.

8.4. Оператор освобождается от обязанности предоставить субъекту персональных данных сведения, предусмотренные п. 8.3 настоящего Положения, в случаях, если:

8.4.1. Субъект персональных данных уведомлен об осуществлении обработки его персональных данных Оператором;

8.4.2. Персональные данные получены Оператором на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;

8.4.3. Персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;

8.4.4. Предоставление субъекту персональных данных сведений, предусмотренных частью 8.3 настоящей Политики, нарушает права и законные интересы третьих лиц.

9. Меры направленные на обеспечение выполнения Оператором обязанностей, предусмотренных Федеральным законом

«О персональных данных»

9.1. Назначен ответственный за организацию обработки персональных данных.

9.2. Изданы документы, определяющие политику Оператора в отношении обработки персональных данных, локальные акты по вопросам обработки персональных данных, локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

9.3. Утверждены правила проведения внутреннего контроля соответствия обработки персональных данных требованиям Федерального закона «О персональных данных» и принятых в соответствии с ним нормативных правовых актов, настоящей Политике, локальным актам.



9.4. Проведена оценка вреда, который может быть причинен субъектам персональных данных, соотношение указанного вреда и применяемых оператором мер.

9.5. Проведено ознакомление работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе документами, определяющими политику Оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных.

#### 10. Меры по обеспечению безопасности персональных данных при их обработке

10.1. Определены угрозы безопасности персональных данных при их обработке в информационных системах персональных данных.

10.2. Применяются 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.

10.3. Применяются прошедшие в установленном порядке процедуру оценки соответствия средства защиты информации.

10.4. Проведена оценка соответствия принимаемых мер по обеспечению безопасности персональных данных, получен аттестат соответствия требованиям по безопасности информации.

10.5. Ведется учет машинных носителей персональных данных.

10.6. Выполняются меры по обнаружению фактов несанкционированного доступа к персональным данным и принятию соответствующих мер.

10.7. Определен комплекс мер по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

10.8. Установлены правила доступа к персональным данным, обрабатываемым в информационных системах персональных данных, обеспечена регистрация и учет всех действий, совершаемых с персональными данными в информационных системах персональных данных.

Осуществляется контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационных систем персональных данных.

#### 11. Порядок управления учетными записями

11.1. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику, допущенному к работе на компьютерах конкретной ИСПДн, должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать на данном компьютере.

11.2. Использование несколькими сотрудниками при работе в ИСПДн одного и того же имени пользователя («группового имени») запрещено.

11.3. Процедура регистрации (создания учетной записи) пользователя и предоставления ему (или изменения его) прав доступа к ресурсам ИСПДн инициируется заявкой ответственного за эксплуатацию данной ИСПДн.

В заявке указывается:

содержание запрашиваемых изменений (регистрация нового пользователя ИСПДн, удаление учетной записи пользователя, расширение или сужение полномочий и прав доступа к ресурсам ИСПДн ранее зарегистрированного пользователя);

должность (с полным наименованием отдела), фамилия, имя и отчество сотрудника;

имя пользователя (учетной записи) данного сотрудника;

полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользователем задач в ИСПДн).

11.4. Заявку рассматривает руководитель, визируя ее, утверждая тем самым производственную необходимость допуска (изменения прав доступа) данного сотрудника к необходимым для решения им указанных в заявке задач ресурсам ИСПДн, затем подписывает задание администратору защиты на внесение необходимых изменений в списки пользователей соответствующих подсистем ИСПДн.

11.5. На основании задания, в соответствии с документацией на средства защиты от несанкционированного доступа, администратор производит необходимые операции по созданию (удалению) учетной записи пользователя, присвоению ему начального значения пароля (возможно также регистрацию персонального идентификатора), заявленных прав доступа к ресурсам ИСПДн и другие необходимые действия, указанные в задании. Для всех пользователей должен быть установлен режим принудительного запроса смены пароля не реже одного раза в течение 90 дней.

11.6. После внесения изменений в списки пользователей администратор информационной безопасности должен обеспечить настройки средств защиты, соответствующие требованиям безопасности указанной ИСПДн. По окончании внесения изменений в списки пользователей в заявке делается отметка о выполнении задания за подписью исполнителя - администратора информационной безопасности.

11.7. Сотруднику, зарегистрированному в качестве нового пользователя ИСПДн, сообщается имя соответствующего ему пользователя и может выдаваться персональный идентификатор (для работы в режиме усиленной аутентификации) и начальное (-ые) значение (-ия) пароля (-ей), которое (-ые) он обязан сменить при первом же входе в систему.

11.8. Исполненные заявка и задание (за подписью администратора информационной безопасности) передаются руководителю на хранение.

Они могут впоследствии использоваться:

- для восстановления полномочий пользователей после аварий ИСПДн;
- для контроля правомерности наличия у конкретного пользователя прав доступа к тем или иным ресурсам ИСПДн при разборе конфликтных ситуаций;
- для проверки сотрудниками контролирурующих органов правильности настройки средств разграничения доступа к ресурсам ИСПДн.

11.9. При наступлении момента прекращения срока действия полномочий пользователя (окончание договорных отношений, увольнение сотрудника) учетная запись должна немедленно блокироваться.