Утверждаю
Директор ТМК ОУ
«Караульская средняя
школа-интернат»
Е.В. Грязева

Положение
«О политике в области обработки и обеспечения безопасности персональных данных в информационных системах персональных данных»

Введение

1. Настоящее положение «О политике в области обработки и обеспечения безопасности персональных данных в информационных системах персональных данных» (далее - Политика), определяет политику в отношении обработки и обеспечения безопасности персональных данных субъектов ТМК ОУ «Караульская средняя школа-интернат» и содержит сведения о реализуемых требованиях к защите персональных данных в Учреждении.
2. Настоящая Политика разработана на основе действующих правовых и нормативных документов по защите конфиденциальной информации и персональных данных.
3. Под персональными данными в настоящем документе понимается любая информация, относящаяся прямо или косвенно, определенному или определяемому физическому лицу (субъекту персональных данных).
4. Настоящая Политика утверждается приказом руководителя Учреждения и подлежит пересмотру по мере необходимости.

1. Общие положения

1.1. Учреждение в рамках выполнения своей деятельности осуществляет обработку персональных данных и, в соответствии с действующим законодательством Российской Федерации, является оператором персональных данных с соответствующими правами и обязанностями, определенными Федеральным законом № 152 от 27.07.2006 г. «О персональных данных» и иными нормативными правовыми актами Российской Федерации (далее - РФ). Состав обрабатываемых данных, категории субъектов, чьи персональные данные обрабатываются Учреждением, цели и правовые основания их обработки закреплены для каждой информационной системы Учреждении, «Перечнем персональных данных, обрабатываемых в ИСПДН.

1.2. Учреждение в установленном порядке проходит регистрацию как оператор персональных данных.

1.3. Учреждение как оператор персональных данных обязано опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных.

1.4. С целью обеспечения выполнения законодательных требований Учреждение считает для себя обязательным обеспечение соответствия обработки персональных данных требованиям законодательства РФ в области защиты информации и персональных данных, и требует аналогичных мер от третьих лиц, которым передаются и (или) могут передаваться персональные данные на основании п.3 Постановления Правительства Российской Федерации от 01 ноября 2012г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.5 Положения настоящей Политики распространяются на весь объем ПДн, обрабатываемых в Учреждении, полученных как до, так и после вступления ее в силу.
1.6. Настоящая Политика вступает в силу с момента ее утверждения руководителем Учреждения и действует бессрочно до замены ее новой Политикой.

2. Принципы, правила и цели обработки персональных данных

2.1. Обработка персональных данных осуществляется Учреждением с соблюдением принципов и правил, предусмотренных Федеральным законом от 27.07.2006 г. №152-ФЗ «О персональных данных»:
- обработка персональных данных осуществляется на законной и справедливой основе;
- обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей;
- обработке подлежат только персональные данные, которые отвечают целям их обработки;
- содержание и объем обрабатываемых персональных данных соответствуют заявленным целям обработки.
- обрабатываемые персональные данные не избыточны по отношению к заявленным целям их обработки;
- при обработке персональных данных обеспечивает точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных;
- Учреждение принимает необходимые меры по удалению или уточнению неполных или неточных данных;
2.3. Обработка персональных данных осуществляется Учреждением только в случаях:
- наличия согласия субъекта персональных данных на обработку его персональных данных, если иное не предусмотрено законодательством РФ;
- наличия заключенного договора, по которому Учреждение обязуется осуществлять обработку персональных данных субъектов по поручению оператора;
- необходимости достижения целей, предусмотренных нормативно-правовыми актами Российской Федерации и трудовым законодательством, для осуществления и выполнения возложенных законодательством РФ на Учреждение функций, полномочий и обязанностей;
- необходимости осуществления прав и законных интересов Учреждения или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;
- обязательного раскрытия и подлежащих к опубликованию персональных данных в соответствии с законодательством РФ;
2.4. Обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. 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. Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя:

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

2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия

от представителя субъекта персональных данных);

3) наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

4) цель обработки персональных данных;

5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;

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

8) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

9) подпись субъекта персональных данных.

2.5. Учреждение обязуется не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации и договором с субъектом.

2.6.Учреждение не обрабатывает специальные и биометричесике категории персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, сведения, характеризующие биологические и физические особенности человека, (данный абзац необходимо рассматривать субъективно для каждой информационной системы персональных данных оператора)

2.7. Учреждение не осуществляет трансграничную передачу персональных данных субъектов персональных данных.

2.8. Учреждение не принимает решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, на основании исключительно автоматизированной обработки его персональных данных.

3. Обработка персональных данных

3.1. Субъектами ПДн в Учреждении являются:

- работники Учреждения, в том числе, кандидаты на вакантные должности;
- обучающиеся, воспитанники Учреждения и их заявители (законные представители).

3.2 Состав обрабатываемых ПДн

3.2.1. В Учреждении обрабатываются ПДн работников и кандидатов на вакантные должности, необходимые в соответствии с Трудовым и Налоговым кодексами Российской Федерации[1].

3.2.2. Полный перечень обрабатываемых ПДн работников и кандидатов на вакантные должности содержится в Перечне обрабатываемых персональных данных, утвержденном директором Учреждения.

3.2.3. В Учреждении обрабатываются ПДн обучающихся, воспитанников и их заявителей (законных представителей), необходимые для осуществления деятельности общеобразовательного учреждения в соответствии с Уставом Учреждения и

---

[1] Наивысшая категория обрабатываемых ПДн работников и кандидатов на вакантные должности – Категория 2, т.е. данные позволяющие идентифицировать субъекта ПДн и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1 (в соответствии с п. 6 Порядка проведения классификации ИСПДн утвержденного приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20)

законодательством РФ в сфере образования, а также для выполнения обязательств и функций, возложенных на Учреждении договорами на содержание обучающихся, воспитанников[2].

3.2.4. Полный перечень обрабатываемых ПДн обучающихся, воспитанников и их заявителей (законных представителей), содержится в Перечне обрабатываемых персональных данных, утвержденном руководителем Учреждения.

3.3 Сроки хранения ПДн

3.3.1. Хранение персональных данных в Учреждении 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, к примеру, Федеральный Закон от 22.10.2004 г. №125-ФЗ «Об архивном деле в Российской Федерации» или договором, стороной которого является субъект персональных данных;

3.3.2. Обрабатываемые персональные данные уничтожаются или обезличиваются по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством РФ.

3.4. Передача ПДн

3.4.1 Учреждение имеет право осуществлять передачу ПДн субъектов ПДн внешним потребителям в следующих случаях:

- субъект ПДн явно выразил свое согласие на такие действия;
- передача ПДн предусмотрена федеральным законом РФ;
- передача происходит в рамках переименования, реорганизации, продажи или иной передачи бизнеса (полностью или части). При этом к приобретателю переходят все обязательства по обеспечению безопасности ПДн.

3.4.2 К внешним потребителям относятся:

- пенсионные фонды (ПФР);
- налоговые инспекции (ИФНС);
- органы социального страхования (ФСС);
- банки;
- медицинские учреждения;
- страховые агентства;
- военкоматы;
- государственные и муниципальные органы управления (УДО);
- Федеральное казначейство;
- Федеральная инспекция труда;
- правоохранительные органы;
- органы лицензирования и сертификации;
- органы статистики;
- органы прокуратуры и ФСБ.

3.5. Общедоступные источники персональных данных

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

---

[2] Наивысшая категория обрабатываемых ПДн обучающихся, воспитанников и их заявителей (законных представителей) – Категория 3, т.е. данные позволяющие идентифицировать субъекта ПДн (в соответствии с п. 6 Порядка проведения классификации ИСПДн утвержденного приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20)

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)
3.5.2. Сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.
(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

4. Обязанности оператора

4.1. При сборе персональных данных оператор обязан предоставить субъекту персональных данных по его просьбе информацию, предусмотренную частью 7 статьи 14 Федерального закона № 152 от 27.07.2006 г. «О персональных данных»
4.2. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.
4.3. Если персональные данные получены не от субъекта персональных данных, оператор, до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:
- наименование либо фамилия, имя, отчество и адрес оператора или его представителя;
- цель обработки персональных данных и ее правовое основание;
- предполагаемые пользователи персональных данных;
- установленные настоящим Федеральным законом права субъекта персональных данных;
- источник получения персональных данных.
4.4. Оператор освобождается от обязанности предоставить субъекту персональных данных сведения, в случаях, если:
- субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим оператором;
- персональные данные получены оператором на основании федерального закона или в связи с исполнением договора, стороной которого либо поручителем по которому является субъект персональных данных;
- персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;
- оператор осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных;
- предоставление субъекту персональных данных сведений, нарушает права и законные интересы третьих лиц.

5. Меры, направленные на обеспечение выполнения Оператором обязанностей, предусмотренных законодательством Российской Федерации

5.1. Учреждение осуществляет следующие организационно-технические меры для защиты персональных данных:
- назначение руководителем Учреждения лица, ответственного за организацию обработки персональных данных;
- издание документов, определяющих политику Учреждения в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;
-применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 Федерального закона №152 «О персональных данных», включая:

- определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных Учреждения;
- применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Учреждения, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;
- применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационных систем персональных данных Учреждения;
- учет машинных носителей персональных данных;
- обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;
- восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установление правил доступа к персональным данным, обрабатываемым в информационных системах персональных данных Учреждении, а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными в информационных системах персональных данных Учреждении;
- контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных Учреждении.
- осуществление внутреннего контроля соответствия обработки персональных данных законодательству Российской Федерации и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике Учреждения в отношении обработки персональных данных, локальным актам Учреждения;
- оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения законодательства Российской Федерации, соотношение указанного вреда и принимаемых Учреждением мер, направленных на обеспечение выполнения обязанностей, предусмотренных законодательством Российской Федерации;
- ознакомление работников Учреждения, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику Учреждения в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.
- доступ к содержанию электронного журнала сообщений возможен исключительно для администратора безопасности, или ответственного за обеспечение безопасности персональных данных в информационных системах Учреждения.

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

6.1. Субъект персональных данных имеет право на получение сведений, указанных в пункте 2.4, за исключением случаев, предусмотренных законодательством в Российской Федерации. Субъект персональных данных вправе требовать от руководителя Учреждения 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 части 2.4. настоящего раздела, предоставляются руководителем Учреждения субъекту персональных данных в доступной форме.

6.3. Сведения, указанные в части 2.4 , предоставляются субъекту персональных данных или его представителю руководителю Учреждения при получении запроса субъекта персональных данных или его представителя в письменной форме.
6.4. В случае, если сведения, указанные в части 2.4, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к руководителю Учреждения или направить в Учреждение повторный запрос в письменной форме в целях получения сведений, указанных в части 2.4, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса.
6.5 Субъект персональных данных вправе обратиться повторно к руководителю Учреждения, или направить повторный письменный запрос в Учреждение в целях получения сведений, указанных в части 2.4, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в части 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 должен содержать обоснование направления повторного запроса.
6.6. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:
- подтверждение факта обработки персональных данных Учреждения;
- правовые основания и цели обработки персональных данных;
- цели и применяемые Учреждением способы обработки персональных данных;
- наименование и место нахождения Учреждения сведения о лицах (за исключением работников Учреждения), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Учреждением или на основании законодательства Российской Федерации;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных законодательством Российской Федерации;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Учреждения, если обработка поручена или будет поручена такому лицу.

7. Обратная связь

7.1. Ответственный за организацию обработки и защиты ПДн в Учреждении: заместитель директора по УВР
7.2. Контактный телефон: 89069007317
7.3.Электронная почта: taimyr 3.1@mail.ru
7.4. Почтовый адрес: 647220, Красноярский край , ул. Северная 2-а
7.5.Все вопросы и предложения по изменению настоящей Политики следует направлять на имя ответственного за организацию обработки и защиты ПДн в Учреждение по указанному выше контактному телефону, почтовому адресу или адресу электронной почты.

Приложение к положению

Правила работы с обезличенными персональными данными Учреждения

1. Общие положения

1.1. Правила работы с обезличенными персональными данными Учреждения (далее - Правила) разработаны с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и постановления Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».
1.2. Настоящие Правила определяют порядок работы с обезличенными данными Учреждения.
1.3. Настоящие Правила утверждаются заведующей Учреждения и действуют постоянно.

2.Условия обезличивания

2.1. Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных Учреждения и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.
2.2. Способы обезличивания при условии дальнейшей обработки персональных данных:
- уменьшение перечня обрабатываемых сведений;
- замена части сведений идентификаторами;
- обобщение - понижение точности некоторых сведений;
- понижение точности некоторых сведений (например, «Место жительства» может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только город);
- деление сведений на части и обработка в разных информационных системах;
другие способы.
2.3. Способом обезличивания в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.
2.4. Для обезличивания персональных данных годятся любые способы явно не запрещенные законодательно.

3. Порядок работы с обезличенными персональными данными

3.1. Обезличенные персональные данные не подлежат разглашению и нарушению Конфиденциальности.
3.2. Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации.
3.3. При обработке обезличенных средств автоматизации необходимо соблюдение:
- парольной политики;
- антивирусной политики;
- правил работы со съемными носителями (если они используется),
- правил резервного копирования;
- правил доступа помещения, где расположены элементы информационных систем;
- иных предусмотренных законодательством Российской Федерации законов и правовых актов.

3.4. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:
- правил хранения бумажных носителей;
- правил доступа к ним и в помещения, где они хранятся;
- иных предусмотренных законодательством Российской Федерации законов и правовых актов.