УТВЕРЖДАЮ
Начальник Управления образования
Администрации муниципального
образования Красноселькупский район

Шарикова А.В.

«___»_____ 20__ г.

ПОЛОЖЕНИЕ

об обработке и обеспечении безопасности персональных данных в Управлении образования Администрации муниципального образования Красноселькупский район

ОГЛАВЛЕНИЕ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых оператором 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.

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств автоматизации оператора.

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

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 оператора персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Глава I. ОБЩИЕ ПОЛОЖЕНИЯ

1. Положение об обработке и обеспечении безопасности персональных данных (далее – Положение) в Управлении образования Администрации муниципального образования Красноселькупский район разработаны на основании требований, установленных:

Трудовым кодексом Российской Федерации;

Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – №152-ФЗ);

Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

Постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

Постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 «Перечень мер направленных на обеспечение выполнения обязанностей предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствие с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

Нормативно-методическими документами Федеральной службы по техническому и экспертному контролю Российской Федерации по обеспечению безопасности ПДн при их обработке в ИСПДн;

2. Оператором персональных данных является Управление образования Администрации муниципального образования Красноселькупский район. Допускается привлекать для обработки персональных данных иные организации (уполномоченные лица) на основе договоров и соглашений.

3. Настоящее Положение устанавливает единый порядок обработки персональных данных в Управлении образования Администрации муниципального образования Красноселькупский район (далее – Управление образования).

4. Действие настоящего Положения распространяется на все процессы по сбору, систематизации, накоплению, хранению, уточнению, использованию, распространению (в том числе передачу), обезличиванию, блокированию, уничтожению ПДн, осуществляемых с использованием средств автоматизации и без их использования.

5. Настоящее Положение вступает в силу с момента его утверждения начальником Управления образования и действует бессрочно, до замены его новым Положением.

6. Все изменения и дополнения в Положение вносятся приказом.

7. Целью настоящего Положения является организация обработки и обеспечения защиты персональных данных граждан от несанкционированного доступа, неправомерного их использования, модификации или их утраты.

8. Обработка персональных данных осуществляется после принятия необходимых мер по защите персональных данных и после получения согласия субъекта персональных данных, за исключением случаев, предусмотренных частью 2 статьи 6 № 152-ФЗ.

9. Лица, допущенные к обработке персональных данных, в обязательном порядке под роспись знакомятся с настоящим Положением и подписывают обязательство о неразглашении информации.

Глава II. ЦЕЛИ, ПОРЯДОК ПОЛУЧЕНИЯ, ДОСТУПА ОБРАБОТКИ И ПЕРЕДАЧИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Порядок получения и обработки персональных данных

10. Получение персональных данных осуществляется в соответствии с нормативно-правовыми актами Российской Федерации в области трудовых отношений и образования, нормативными и распорядительными документами Минобрнауки России и Рособразования, настоящим Положением на основе трудовых договоров или письменного согласия субъектов персональных данных.

11. 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 Федеральным законом от 27.07.2006 № 152-ФЗ "О персональных данных".

12. Без согласия субъектов осуществляется обработка общедоступных персональных данных или содержащих только фамилии, имена и отчества, обращений и запросов организаций и физических лиц, регистрация и отправка корреспонденции почтовой связью, оформление разовых пропусков, обработка персональных данных для исполнения трудовых договоров или без использования средств автоматизации и в иных случаях, предусмотренных законодательством Российской Федерации.

13. Обработка и использование персональных данных осуществляется в целях, указанных в соглашениях с субъектами персональных данных, а также в случаях, предусмотренных нормативно-правовыми актами Российской Федерации и настоящим Положением. Не допускается принятие на основании исключительно автоматизированной

обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы.

14. В случае увольнения субъекта персональных данных и иного достижения целей обработки персональных данных, зафиксированных в письменном соглашении, Оператор обязан незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий трех рабочих дней с даты достижения цели обработки персональных данных, если иное не предусмотрено законодательством и настоящим Положением.

Цели обработки персональных данных

15. Целью обработки персональных данных является:

выполнение постановления Правительства РФ от 27.01.2012 г. № 36 «Об утверждении правил формирования и ведения федеральной информационной системы обеспечения проведения единого государственного экзамена и приема граждан в образовательные учреждения среднего профессионального образования и образовательные учреждения высшего профессионального образования и региональных информационных систем обеспечения проведения единого государственного экзамена», а также в рамках региональной программы «Сетевой город. Образование»;

осуществления возложенных на Управление образования законодательством функций, полномочий и обязанностей, а также для реализации права на труд, права на пенсионное обеспечение и медицинское страхование.

16. Руководство Управления образования вправе разрешать доступ к персональным данным, только специально уполномоченным лицам, в соответствии с утвержденной матрицей доступа субъектов ИСПДн «УО Красноселькуп» к ее защищаемым информационным ресурсам.

Доступ к персональным данным

17. Управление образования обеспечивает конфиденциальность персональных данных субъектов ПДн, то есть не допускает их распространение без согласия субъекта персональных данных или наличия иного законного основания (в том числе по иным основаниям, предусмотренным ч.1 ст.6 Федерального закона №152-ФЗ «О персональных данных»), за исключением случаев обезличенных персональных данных и в отношении общедоступных персональных данных.

18. В отношении персональных данных субъектов вводится режим ограничения доступа. Доступ к персональным данным субъекта имеют только те работники Управления

образования, которым персональные данные необходимы в связи с исполнением ими трудовых обязанностей и только в необходимом объеме.

19. Руководство Управления образования вправе разрешать доступ к персональным данным, только специально уполномоченным лицам, в соответствии с утвержденной начальником Управления образования матрицей доступа субъектов ИСПДн «УО Красноселькуп» к ее защищаемым информационным ресурсам. Форма матрицы доступа субъектов к ее защищаемым информационным ресурсам приведена в приложении 5 настоящего Положения.

20. Субъект ПДн имеет право на свободный доступ к своим персональным данным, включая право на получение копии любой записи, содержащей его персональные данные (за исключением случаев, предусмотренных ч.8 ст.14 Федерального закона №152-ФЗ «О персональных данных»). Субъект имеет право вносить предложения по внесению изменений в свои данные в случае обнаружения в них неточностей.

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

подтверждение факта обработки персональных данных Управление образования;

правовые основания и цели обработки персональных данных;

цели и применяемые способы обработки персональных данных;

наименование и место нахождения Управления образования, сведения о лицах (за исключением работников Управления образования), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Управлением образования или на основании федерального закона;

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 настоящим Федеральным законом;

информацию об осуществленной или о предполагаемой трансграничной передаче данных;

наименование и адрес организации, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена сторонней организации;

иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами.

22. Доступ к своим персональным данным предоставляется субъекту ПДн или его законному представителю при обращении, либо при получении запроса субъекта персональных данных или его законного представителя.

Передача персональных данных

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

24. Передача персональных данных государственному казённому учреждению Ямало-Ненецкого автономного округа «Региональный центр оценки качества образования» и в другие информационные системы, входящие в информационную систему «УО Красноселькуп» осуществляется только по установленному VPN каналу с применением криптографических средств защиты информации.

25. Ответы на правомерные письменные запросы учреждений и организаций даются с разрешения начальника Управления образования и только в письменной форме и в том объеме, который позволяет не разглашать излишний объем персональных сведений.

26. Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.

27. По возможности персональные данные обезличиваются.

Глава III. КАТЕГОРИЯ СУБЪЕКТОВ

28. К субъектам, персональные данные которых обрабатываются, относятся:

граждане проходящие (прошедшие) обучение в общеобразовательных учреждениях ЯНАО;

граждане, состоящие в настоящем времени в трудовых отношениях с Управлением образования.

29. К субъектам, которые обрабатывают персональные данные, относятся:

Администратор ИСПДн – сотрудник Управления образования, ответственный за настройку, внедрение и сопровождение ИСПДн. Обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (оператора АРМ) к элементам, хранящим персональные данные.

Администратор безопасности – сотрудник Управления образования, ответственный за функционирование СЗПДн, включая обслуживание и настройку административной, серверной и клиентской компонент.

Оператор АРМ (Пользователь) – сотрудник Управления образования, осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПД. Оператор не имеет полномочий для управления подсистемами обработки данных и СЗПДн. Обладает правами, определенными матрицей прав доступа к ИСПДн.

Глава IV. ПРОЦЕДУРЫ, НАПРАВЛЕННЫЕ НА ВЫЯВЛЕНИЕ И ПРЕДОТВРАЩЕНИЕ НАРУШЕНИЙ ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Меры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации

30. Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, а также используемые в информационной системе информационные технологии.

31. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

32. К мерам, направленным на выявление и предотвращение нарушений законодательства Российской Федерации в сфере обработки персональных данных относятся:

назначение ответственного за организацию обработки персональных данных;

применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии с частями 1 и 2 статьи 19 № 152-ФЗ;

осуществление внутреннего контроля соответствия обработки персональных данных № 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

оценка вреда, который может быть причинён субъектам персональным данных в случае нарушения законодательства Российской Федерации и настоящего Положения;

ознакомление работников, непосредственно осуществляющих обработку персональных данных с положениями законодательства Российской Федерации о персональных данных и настоящим Положением;

запрет на обработку персональных данных лицами, не допущенными к их обработке.

Защита персональных данных

33. Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

34. Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

35. Защита персональных данных представляет собой жестко регламентированный и динамически-технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности.

36. Защита персональных данных от неправомерного их использования или утраты должна быть обеспечена в порядке, установленном федеральными законами и организационно-распорядительными документами Управления образования в области защиты информации.

37. Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителями и специалистами.

38. Для обеспечения внутренней защиты персональных данных необходимо соблюдать ряд мер:

ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;

строгое избирательное и обоснованное распределение документов и информации между работниками;

рациональное размещение рабочих мест работников, исключающее бесконтрольное использование защищаемой информации;

знание работником требований нормативно-методических документов по защите информации и сохранении тайны;

наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;

определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;

организация порядка уничтожения информации;

своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения;

воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами.

39. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

40. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности Управления образования, посетители, работники других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов, содержащих конфиденциальную информацию.

41. Для обеспечения внешней защиты персональных данных необходимо соблюдать ряд мер:

порядок приема, учета и контроля деятельности посетителей;

пропускной режим организации;

учет и порядок выдачи удостоверений;

технические средства охраны, сигнализации;

порядок охраны территории, зданий, помещений, транспортных средств;

требования к защите информации при интервьюировании и собеседованиях.

42. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных.

43. По возможности персональные данные обезличиваются.

44. Кроме мер защиты персональных данных, установленных законодательством, сотрудники Управления образования и их представители могут вырабатывать совместные меры защиты персональных данных.

Порядок обработки персональных данных в информационных системах персональных данных с использованием средств автоматизации

45. Обработка персональных данных в информационных системах персональных данных осуществляется после завершения работ по созданию системы защиты персональных данных в информационной системе, комиссионной ее проверки, и оценки соответствия информационной системы персональных данных требованиям безопасности информации.

46. Обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации осуществляется в соответствии с требованиями Постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативных и руководящих документов уполномоченных федеральных органов исполнительной власти.

47. Безопасность персональных данных, обрабатываемых с использованием средств автоматизации, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным.

48. Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации организационных мер и путем применения программных и технических средств.

49. Самостоятельное подключение средств вычислительной техники, применяемых для хранения, обработки или передачи персональных данных, к информационно-телекоммуникационным сетям, позволяющим осуществлять передачу информации через государственную границу Российской Федерации, в том числе к информационно-телекоммуникационной сети Интернет, не допускается.

50. Доступ пользователей к персональным данным в информационных системах персональных данных разрешается после обязательного прохождения процедуры идентификации и аутентификации.

51. При эксплуатации автоматизированных систем необходимо соблюдать требования:

к работе допускаются только назначенные лица;

на ПЭВМ, дисках, папках и файлах, на которых обрабатываются и хранятся сведения о персональных данных, должны быть установлены пароли (идентификаторы);

на период обработки защищаемой информации в помещении могут находиться лица, допущенные в установленном порядке к обрабатываемой информации.

52. Не допускается обработка персональных данных в ИСПДн с использованием средств автоматизации при отсутствии:

утвержденных организационно-технических документов о порядке эксплуатации информационных систем персональных данных, включающих акт классификации ИСПДн, инструкции пользователя, администратора по организации антивирусной защиты, парольной защиты автоматизированных систем, и других нормативных и методических документов;

настроенных средств защиты от несанкционированного доступа, средств антивирусной защиты, резервного копирования информации и других программных и технических средств в соответствии с требованиями безопасности информации;

охраны и организации режима допуска в помещения, предназначенные для обработки персональных данных.

53. Должностными лицами, ответственными за обеспечение безопасности персональных данных при их обработке в информационных системах, должно быть обеспечено:

своевременное обнаружение фактов несанкционированного доступа к персональным данным и немедленное доведение этой информации до руководящих должностных лиц;

недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

постоянный контроль за обеспечением уровня защищенности персональных данных;

знание и соблюдение условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

при обнаружении нарушений порядка предоставления персональных данных незамедлительное приостановление предоставления персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин;

разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработка и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

54. В случае выявления нарушений порядка обработки персональных данных в информационных системах уполномоченными должностными лицами принимаются меры по установлению причин нарушений и их устранению.

Порядок обработки персональных данных без использования средств автоматизации

55. Обработка персональных данных без использования средств автоматизации (далее – неавтоматизированная обработка персональных данных) может осуществляться в виде документов на бумажных носителях и в электронном виде (файлы, базы банных) на электронных носителях информации.

56. При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

57. При неавтоматизированной обработке персональных данных на бумажных носителях:

не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо несовместимы;

персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);

документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных;

дела с документами, содержащими персональные данные, должны иметь внутренние описи документов с указанием цели обработки и категории персональных данных.

58. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее – типовые формы), должны соблюдаться следующие условия:

типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных;

типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо несовместимы.

59. Документы и внешние электронные носители информации, содержащие персональные данные, должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

60. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных, с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

61. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

62. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, – путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

63. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

64. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

Глава V. ПЕРЕЧЕНЬ И ОБЯЗАННОСТИ ДОЛЖНОСТЫХ ЛИЦ, ОТВЕТСТВЕННЫХ ЗА ОБРАБОТКУ И ОБЕЗЛИЧИВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

65. Работники Управления образования допускаются к обработке персональных данных и имеют доступ к персональным данным в случае замещениями ими должностей:

начальника Управления образования;

заместителя начальника Управления образования;

начальника службы системных администраторов;

инженера по защите информации;

инспектора по кадрам.

66. Перечень должностей, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных:

заместитель начальника Управления образования;

начальник службы системных администраторов;

инженер по защите информации;

инспектор по кадрам.

67. Лица, допущенные к обработке персональных данных, в обязательном порядке под роспись знакомятся с настоящим Положением и подписывают обязательство о неразглашении информации, содержащей персональные данные, являющимся Приложением № 1 к настоящему Положению.

68. Ответственный за организацию обработки персональных данных в местной администрации назначается распоряжением начальника Управления образования из числа сотрудников Управления образования.

69. Лица, замещающие должности, указанные в статье 65 настоящего Положения в случае расторжения с ним контракта (договора), дают письменное обязательство прекратить обработку персональных данных, ставших известными им в связи с исполнением должностных обязанностей.

70. Обязательство о прекращении обработки персональных данных даётся в письменной форме согласно Приложения № 2 к настоящему Положению.

71. Оператор перед обработкой персональных данных получает у субъектов обработки персональных данных согласие на обработку их персональных данных.

72. Согласие на обработку персональных данных даётся субъектом обработки персональных данных в письменной форме.

Типовая форма согласия на обработку персональных данных является Приложением № 3 к настоящему Положению.

73. В случае отсутствия согласия на обработку персональных данных оператор разъясняет субъекту обработки персональных данных юридические последствия отказа предоставить свои персональные данные. Разъяснение юридических последствий осуществляется в письменной форме согласно Приложению № 4 к настоящему Положению.

Глава VI. ПОРЯДОК ИСПОЛЬЗОВАНИЯ, ОБРАБОТКИ И ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

Использование персональных данных

74. В Управлении образования не осуществляется принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы.

Сроки обработки и хранения обрабатываемых персональных данных

75. Сроки обработки и хранения персональных данных определяются:

достижением цели обработки персональных данных;

решением субъекта;

положениями письма Минобразования РФ от 20.12.2000 № 03-51/64;

иными требованиями законодательства Российской Федерации, региональными и ведомственными нормативно-правовыми актами.

Порядок хранения персональных данных

76. Хранение персональных данных должно осуществляться 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.

77. При хранении персональных данных субъектов ПДн применяются средства защиты от несанкционированного доступа.

Порядок учета машинных носителей информации

78. В Управлении образования ведется учет машинных носителей информации, содержащей ПДн.

79. Кандидатура работника, на которого планируется возложить обязанности по учету носителей с ПДн, назначается приказом начальника Управления образования.

80. В процессе первоначального учета составляется перечень имеющихся машинных носителей ПДн с указанием состава имеющихся на них ПДн.

81. Каждому носителю ПДн присваивается учетный номер. Для этого все носители должны быть промаркированы печатью или наклейкой с учетным номером. На носители (компакт-диски и др.), на которые наклеивание ярлыка недопустимо по техническим причинам, реквизиты ярлыка полностью наносятся на диск специальным нестираемым маркером.

82. После присвоения учетного номера осуществляется регистрация носителя в Журнале учета машинных носителей ПДн.

83. Ведение Журнала возлагается на назначенного работника.

84. В Управлении образования ежегодно проводится инвентаризация машинных носителей информации, на которых хранятся ПДн.

Глава VII. ПОРЯДОК УНИЧТОЖЕНИЯ ОБРАБОТАННЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

85. Под уничтожением обработанных персональных данных понимаются действия, в результате которых невозможно восстановить содержание персональных данных в

информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

86. Персональные данные субъектов ПДн подлежат уничтожению, если иное не предусмотрено федеральными законами или соглашением между Управлением образования и субъектом персональных данных, в следующих случаях:

по достижении целей обработки или в случае утраты необходимости в их достижении;

в случае отзыва субъектом персональных данных согласия на обработку своих персональных данных (за исключением случаев предусмотренных ч.5 ст.6 Федерального закона № 152-ФЗ «О персональных данных»);

в случае выявления неправомерных действий с персональными данными и невозможностью устранения допущенных нарушений в срок, установленным законодательством.

87. В случае если проведение мероприятий по уничтожению ПДн не представляется возможным в связи с технологией обработки этих ПДн, необходимо провести мероприятия по обезличиванию указанных ПДн.

88. Персональные данные должны уничтожаться с машинных носителей, бумажных носителей и в ИСПДн, в которых они обрабатываются.

89. Уничтожение обработанных персональных данных производится комиссионно с составлением соответствующего акта.

Глава VIII. ПРАВИЛА РАССМОТРЕНИЯ ЗАПРОСОВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

90. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, указанной в части 7 статьи 14 № 152-ФЗ, в том числе содержащей:

подтверждение факта обработки персональных данных в Управлении образования;

правовые основания и цели обработки персональных данных;

цели и применяемые в Управлении образования способы обработки персональных данных;

сведения о лицах (за исключением работников Управления образования), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Управлением образования или на основании федерального закона;

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 настоящим Федеральным законом;

информацию об осуществленной или о предполагаемой трансграничной передаче данных;

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

иные сведения, предусмотренные Федеральным законом или другими федеральными законами.

91. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с частью 8 статьи 14 № 152-ФЗ.

92. Субъект персональных данных имеет право 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.

93. Сведения, указанные в части 7 статьи 14 № 152-ФЗ, должны быть предоставлены субъекту персональных данных 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.

94. Сведения предоставляются субъекту персональных данных или его представителю при обращении либо при получении запроса субъекта персональных данных или его представителя.

95. Запрос регистрируется в день поступления по правилам делопроизводства.

96. Запрос субъекта персональных данных должен содержать сведения позволяющие провести его идентификацию:

фамилию, имя, отчество субъекта персональных данных и его представителя;

адрес проживания субъекта персональных данных и его представителя;

номер и дату выдачи основного документа, подтверждающего личность субъекта персональных данных и его представителя;

подпись субъекта персональных данных и его представителя.

97. Запрос может быть направлен электронной почтой и подписан электронной подписью в соответствии с законодательством Российской Федерации.

98. Рассмотрение запросов является служебной обязанностью начальника, заместителей начальника и уполномоченных должностных лиц, в чьи обязанности входит обработка персональных данных.

99. Должностные лица Управления образования обеспечивают:

объективное, всестороннее и своевременное рассмотрения запроса;

принятие мер, направленных на восстановление или защиту нарушенных прав, свобод и законных интересов субъектов персональных данных;

направление письменных ответов по существу запроса.

100. Оператор при получении запроса субъекта персональных данных или его представителя, а также уполномоченного органа по защите прав субъектов персональных данных обязан сообщить в порядке статьи 14 № 152-ФЗ 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 в течении 30 (тридцати) дней с даты получения запроса.

101. Запрос проверяется на повторность, при необходимости сверяется с находящейся в архиве предыдущей перепиской. В случае если сведения, указанные в части 7 статьи 14 № 152-ФЗ, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в Управление образования или направить повторный запрос в целях получения сведений, указанных в части 7 статьи 14 № 152-ФЗ, 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.

102. Субъект персональных данных вправе обратиться повторно в Управление образования или направить повторный запрос в целях получения сведений, указанных в части 7 статьи 14 № 152-ФЗ, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в настоящем пункте, 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 с необходимыми сведениями должен содержать обоснование направления повторного запроса.

103. Прошедшие регистрацию запросы в тот же день докладываются начальнику Управления образования либо лицу, его заменяющему, который определяет порядок и сроки их рассмотрения, дает по каждому из них письменное указание исполнителям.

104. Управление образования вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным частями 4 и 5 статьи 14 Федерального закона. Такой отказ должен быть мотивированным.

105. В случае отказа в предоставлении информации о наличии персональных данных оператор обязан дать в письменной форме мотивированный ответ со ссылкой на действующее законодательство, являющегося основанием для такого отказа. Отказ в предоставлении информации направляется в срок, не превышающий 30 (тридцати) дней со дня получения запроса субъекта персональных данных.

106. В случае предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор в срок, не превышающий 7 (семь) рабочих дней, вносит в них необходимые изменения. О внесённых изменениях уведомляется субъект персональных данных или его представитель.

107. В случае выявления неправомерной обработки персональных данных уполномоченные должностные лица Управления образования в срок, не превышающий 3 (трех) рабочих дней с даты этого выявления, обязаны прекратить неправомерную обработку персональных данных. В случае если обеспечить правомерность обработки персональных данных, невозможно, уполномоченные должностные лица Управления образования в срок, не превышающий 10 (десяти) рабочих дней с даты выявления неправомерной обработки персональных данных, обязаны уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Управление образования обязано уведомить субъекта персональных данных или его представителя, 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.

108. Для проверки фактов, изложенных в запросах, при необходимости организуются служебные проверки в соответствии с законодательством Российской Федерации. По

результатам служебной проверки составляется мотивированное заключение, которое должно содержать объективный анализ собранных материалов. Если при проверке выявлены факты совершения работниками Управления образования действия (бездействия), содержащего признаки административного правонарушения или состава преступления информация передается незамедлительно в правоохранительные органы. Результаты служебной проверки докладываются начальнику Управления образования.

109. При получении запроса из уполномоченного органа по защите прав субъектов персональных данных оператор обязан сообщить необходимую информацию в течении 30 (тридцати) дней с даты получения такого запроса.

110. Возможность ознакомления с персональными данными предоставляется на безвозмездной основе лицом ответственным за обработку персональных данных.

111. Запрос считается исполненным, если рассмотрены все поставленные в нем вопросы, приняты необходимые меры и даны исчерпывающие ответы заявителю.

112. Ответы на запросы печатаются на бланке установленной формы и регистрируются за теми же номерами, что и запросы.

113. Начальник Управления образования осуществляет непосредственный контроль за соблюдением установленного законодательством РФ и настоящих Правил.

Глава IX. ПРАВИЛА РАБОТЫ С ОБЕЗЛИЧЕННЫМИ ДАННЫМИ

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

115. Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса используемых информационных систем персональных данных и по достижению сроков обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законодательством Российской Федерации.

116. К способам обезличивания персональных данных в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.

117. К способам обезличивания персональных данных при условии дальнейшей обработки персональных данных относятся:

уменьшение перечня обрабатываемых сведений;

замена части сведений идентификаторами;

обобщение (понижение) точности некоторых сведений;

деление сведений на части и обработка их в разных информационных системах;

другие способы.

118. Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

119. Обезличенные персональные данные могут обрабатываться с использования и без использования средств автоматизации.

120. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо:

использование паролей;

использование антивирусных программ;

правил работы со съемными носителями (если они используется);

правил резервного копирования;

соблюдение правил доступа в помещение, в котором ведётся обработка персональных данных.

121. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

хранения бумажных носителей в условиях, исключающих доступ к ним посторонних лиц;

соблюдение правил доступа в помещение, в котором ведётся обработка персональных данных.

Глава X. ПРАВИЛА ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ

122. Внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных осуществляется с целью проверки соответствия обработки персональных данных требованиям к защите персональных данных, установленных № 152-ФЗ, принятыми в соответствии с ним нормативными правовыми актами и локальными актами оператора.

123. Текущий контроль осуществляется на постоянной основе ответственным за обработку персональных данных в ходе мероприятий по обработке персональных данных.

124. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям руководство Управления образования организует проведение периодических проверок условий обработки персональных данных.

125. Проверки осуществляются ответственным за организацию обработки персональных данных либо комиссией, назначаемой начальником Управления образования. Периодичность проверки – не реже одного раза в год.

126. В проведении проверки не может участвовать лицо, прямо или косвенно заинтересованное в её результатах.

127. При проведении внутренней проверки соответствия обработки персональных данных с использованием средств автоматизации установленным требованиям комиссией должны быть полностью, объективно и всесторонне установлены:

порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке;

эффективность принимаемых мер по обеспечению безопасности персональных данных;

соответствие полномочий пользователя матрице доступа;

соблюдение пользователями информационных систем персональных данных парольной политики;

соблюдение пользователями информационных систем персональных данных антивирусной политики;

порядок и условия применения средств защиты информации;

состояние учёта машинных носителей персональных данных и соблюдение пользователями информационных систем персональных данных правил работы с ними;

наличие (отсутствие) фактов несанкционированного доступа к персональным данным;

мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

соблюдение порядка доступа в помещения, где расположены элементы информационных систем персональных данных;

соблюдение порядка резервирования баз данных и хранения резервных копий.

128. При проведении внутренней проверки соответствия обработки персональных данных без использования средств автоматизации установленным требованиям комиссией должны быть полностью, объективно и всесторонне установлены:

порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных;

хранение бумажных носителей с персональными данными;

доступ к бумажным носителям с персональными данными;

доступ в помещения, где обрабатываются и хранятся бумажные носители с персональными данными.

129. Проверки осуществляются непосредственно на месте обработки персональных данных путем опроса и осмотра рабочих мест сотрудников, участвующих в процессе обработки персональных данных.

130. Срок проведения проверки не может составлять более 30 (тридцати) дней со дня принятия решения о её проведении.

131. Результаты проверки оформляются в виде письменного заключения (акта), утверждаются председателем комиссии и докладываются начальнику Управления образования.

132. Выявленные в ходе проверки нарушения, оформляются в форме плана мероприятий по устранению выявленных недостатков с указанием сроков исполнения.

133. Акты и планы устранения выявленных недостатков хранятся у ответственного за организацию обработки персональных данных в течение года.

134. В отношении персональных данных, ставших известными комиссии в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных.

Глава XI. ПОРЯДОК ДОСТУПА В ПОМЕЩЕНИЯ, В КОТОРЫХ ВЕДЕТСЯ ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

135. Запрещается оставлять материальные носители с персональными данными без присмотра в незапертом помещении, в котором осуществляется обработка персональных данных.

136. Допуск сотрудников Управления образования, постоянно работающих в служебных помещениях, в которых ведется обработка персональных данных и размещены аппаратные СЗИ, осуществляется соответствующим приказом.

137. В служебных помещениях, занимаемых Управлением образования, применяются административные, технические, физические и процедурные меры, направленные для защиты данных от нецелевого использования, несанкционированного доступа, раскрытия, потери, изменения и уничтожения обрабатываемых персональных данных.

138. К мерам защиты данных от нецелевого использования относятся:

физические меры защиты: двери, снабжённые замками; сейфы; безопасное уничтожение носителей, содержащих персональные данные;

технические меры защиты: применение антивирусных программ, программ защиты; установление паролей на персональных компьютерах;

организационные меры защиты: обучение и ознакомление с принципами безопасности и конфиденциальности; доведение до операторов обработки персональных данных важности защиты персональных данных и способов обеспечения защиты.

Глава XII. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, СВЯЗАННОЙ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

139. Персональная ответственность - одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

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

141. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

142. Каждый сотрудник организации, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

143. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

144. За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера работодатель вправе применять предусмотренные Трудовым кодексом дисциплинарные взыскания.

145. Должностные лица, в обязанность которых входит ведение персональных данных сотрудника, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации - влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.

146. В соответствии с Гражданским кодексом лица, незаконными методами получившие информацию, составляющую служебную тайну, обязаны возместить причиненные убытки, причем такая же обязанность возлагается и на работников.

147. Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения наказывается штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью, либо арестом в соответствии с УК РФ.

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

Заместитель начальника Управления образования

С.Б. Багрова

«___»_____20__ г.

Приложение № 1
к Положению...

ОБЯЗАТЕЛЬСТВО

о неразглашении информации, содержащей персональные данные

Я, _____,

(фамилия, имя, отчество лица, допущенного к обработке персональных данных)

исполняющий (-ая) должностные обязанности по замещаемой должности

_____

предупрежден (-а) о том, что на период исполнения должностных обязанностей мне будет предоставлен допуск к информации, содержащей персональные данные.

Настоящим добровольно принимаю на себя обязательства:

1. Не передавать и не разглашать третьим лицам информацию, содержащую персональные данные, которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей.

2. В случае попытки третьих лиц получить от меня информацию, содержащую персональные данные, сообщать непосредственному начальнику.

3. Не использовать информацию, содержащую персональные данные, с целью получения выгоды.

4. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты персональных данных.

5. В случае расторжения договора (контракта) и (или) прекращения права на допуск к информации, содержащей персональные данные, не разглашать и не передавать третьим лицам известную мне информацию, содержащую персональные данные.

Я предупрежден (а) о том, что нарушение данного обязательства является основанием привлечения к дисциплинарной ответственности и (или) иной ответственности в соответствии с законодательством Российской Федерации.

Ознакомлен: «___» _____ 20__ г. _____ _____

(подпись) *(расшифровка подписи)*

Приложение № 2
к Положению ...

ОБЯЗАТЕЛЬСТВО
о прекращении обработки персональных данных лица, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним контракта

Я _____

(фамилия, имя, отчество)

_____

(должность)

обязуюсь прекратить обработку персональных данных, ставших известными мне в связи с исполнением должностных обязанностей, в случае расторжения со мной контракта (договора), освобождения меня от замещаемой должности и увольнения.

В соответствии со статьей 7 Федерального закона от 27 июля 2006 №152-ФЗ «О персональных данных» я уведомлен (-а) о том, что персональные данные являются конфиденциальной информацией и я обязан (а) не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, ставших известными мне в связи с исполнением должностных обязанностей.

Ответственность, предусмотренная Федеральным законом от 27 июля 2006 № 152-ФЗ «О персональных данных» и законодательством Российской Федерации, мне разъяснена.

«___» _____ 20__ г. _____ _____

(подпись) *(расшифровка подписи)*

Приложение № 3
к Положению...

ФОРМА
согласия на обработку персональных данных

Я, _____,

(фамилия, имя, отчество)

зарегистрированный по адресу: _____,

паспорт серия _____ номер_____ выдан «_____» _____ _____г.

_____,

(наименование органа выдавшего документ)

в соответствии со статьёй 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» своей волей и в своем интересе с целью решения вопросов местного значения даю согласие оператору – Управлению образования Администрации муниципального образования Красноселькупский район на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных. А именно:

анкетные и биографические данные гражданина, включая адрес места жительства и проживания;

паспортные данные или данные иного документа, удостоверяющего личность и гражданство, включая серию, номер, дату выдачи, наименование органа, выдавшего документ);

сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки, включая серию, номер, дату выдачи диплома, свидетельства, аттестата или другого документа об окончании образовательного учреждения, дату начала и завершения обучения);

сведения о трудовой деятельности, опыте работы, занимаемой должности, трудовом стаже, повышения квалификации и переподготовки, включая сведения о номере, серии, дате выдачи трудовой книжки (вкладыша в неё) и записях в ней, содержание и реквизиты трудового договора (контракта);

сведения о составе семьи и наличии иждивенцев, сведения о месте работы или учёбы членов семьи;

сведения о состоянии здоровья и наличии заболеваний (когда это необходимо в случаях, установленных законодательством);

сведения об отношении к воинской обязанности;

сведения о доходах и обязательствах имущественного характера, в том числе членов семьи;

сведения об идентификационном номере налогоплательщика;

сведения о социальных льготах и о социальном статусе;

сведения из страховых полисов обязательного (добровольного) медицинского страхования;

сведения о номере и серии страхового свидетельства государственного пенсионного страхования.

Если мои персональные данные можно получить только у третьей стороны, то я должен быть уведомлен об этом заранее с указанием целей, предполагаемых источников и способов получения персональных данных, также должно быть получено на это согласие.

Мне разъяснены мои права и обязанности, связанные с обработкой персональных данных, в том числе, моя обязанность проинформировать оператора в случае изменения моих персональных данных; мое право в любое время отозвать свое согласие путем направления соответствующего письменного заявления оператору.

Согласие вступает в силу со дня его подписания и действует в течение неопределенного срока до достижения цели обработки персональных данных или его отзыва в письменной форме.

«___» _____ 20__ г. _____ _____

(подпись) *(расшифровка подписи)*

Приложение № 4
к Положению...

ФОРМА
разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные

Мне, _____,

(фамилия, имя, отчество)

разъяснены юридические последствия отказа предоставить свои персональные данные оператору - Управлению образования Администрации муниципального образования Красноселькупский район.

В соответствии с Постановлением Правительства Российской Федерации от 21.03.2012 г. № 211 «Перечень мер направленных на обеспечение выполнения обязанностей предусмотренных Федеральным законом «О персональных данных», статьей 28 Положения об обработке и обеспечении безопасности персональных данных в Управлении образования Администрации муниципального образования Красноселькупский район определён перечень персональных данных, которые субъект персональных данных обязан предоставить в связи с осуществлением возложенных на Управление образования федеральным законодательством функций, полномочий и обязанностей, а также для реализации права на труд, права на пенсионное обеспечение и медицинское страхование.

Я предупрежден, что в случае несогласия на обработку моих персональных данных:

1. Администрацией Управления образования при решении вопросов местного значения мои права могут быть реализованы не в полном объеме.

2. Право на труд, право на пенсионное обеспечение и медицинское страхование работников не может быть реализовано в полном объёме, а трудовой договор (контракт) подлежит расторжению.

«___» _____ 20__ г. _____ _____

(подпись) *(расшифровка подписи)*

Приложение№5
к Положению…

УТВЕРЖДАЮ
Начальник Управления образования
Администрации муниципального образования
Красносельскупский район

Шарикова А. В.
«___»_____ 20__ г.

МАТРИЦА ДОСТУПА

субъектов автоматизированной системы ИСПДн «УО Красносельскуп» к ее защищаемым информационным ресурсам

№ п/п	Наименование АРМ	Здание, № помещения	Условное имя пользователя (группы)/ ФИО	Наименование защищаемых ресурсов (логические диски, каталоги, программы, устройства и т.п.)	Тип доступа	Примечание
1	АРМ 1	Тверская 12, к 212	Администратор/ Иванов И.И.	C:\Каталог 1	чтение	
					запись	
					выполнение	
				C:\Каталог 2	чтение	
					запись	
					выполнение	
				FDD	чтение	
					запись	
					выполнение	
				Сканер	сканирование	
				DVD-RW	чтение	
					запись	
					выполнение	
				Принтер	печать	
				Программные средства	инсталляция, изменение	
				ОС, СЗИ	настройки	
2	АРМ 2	Тверская 12, к 310	Пользователь/ Петров П.П.	C:\Каталог 1	чтение	
					запись	
				Принтер	печать	
				Программные средства	выполнение	
				ОС, СЗИ	загрузка	

«___» _____ 20__ г. _____ _____

(подпись) (расшифровка подписи)

ЛИСТ ОЗНАКОМЛЕНИЯ

№ п.п.	Должность	ФИО	Дата	Подпись
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				
20.				
21.				
22.				
23.				
24.				
25.				
26.				
27.				
28.				

№ п.п.	Должность	ФИО	Дата	Подпись
29.				
30.				
31.				
32.				
33.				
34.				
35.				
36.				
37.				
38.				
39.				
40.				
41.				
42.				
43.				
44.				
45.				
46.				
47.				
48.				
49.				
50.				
51.				
52.				
53.				
54.				
55.				
56.				