

Приложение 3
Утверждено
приказом управления образования
от 20.03.2020 г. № 01.01-ОД

РЕГЛАМЕНТ
управления образования администрации Косинского
муниципального округа Пермского края в отношении
обработки и обеспечения безопасности персональных данных

1. Общие положения

Регламент управления образования администрации Косинского муниципального округа Пермского края в отношении обработки и обеспечения безопасности персональных данных (далее – Регламент) принят в целях защиты информации, в отношении которой установлено требование об обеспечении ее конфиденциальности, в том числе персональных данных (далее – ПДн), обрабатываемых в управлении образования администрации Косинского муниципального округа Пермского края (далее – Управление).

Регламент определяет права и обязанности сотрудников Управления, порядок использования указанных данных в служебных целях, а также порядок обработки ПДн.

Настоящий Регламент разработан на основе и во исполнение части 1 статьи 23, статьи 24 Конституции Российской Федерации, пункта 2 и 3 части 1 статьи 18.1 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ), Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Положения Регламента распространяются на отношения по обработке и защите ПДн, полученных Управлением как до, так и после утверждения Регламента, за исключением случаев, когда по причинам правового, организационного и иного характера положения Регламента не могут быть распространены на отношения по обработке и обеспечению безопасности ПДн, полученных до его утверждения. Лица из числа сотрудников Управления, уполномоченные на обработку ПДн, обеспечивающие обработку ПДн в соответствии с требованиями Федерального закона № 152-ФЗ, других правовых актов Российской Федерации и несущих ответственность в соответствии с законодательством Российской Федерации за нарушение мер по обеспечению безопасности этих ПДн, назначаются приказами начальника Управления.

Если в отношениях с Управлением участвуют законные представители субъектов ПДн, то Управление становится оператором ПДн лиц, представляющих указанных субъектов. Положения Регламента и другие локальные акты Управления распространяются на случаи обработки и обеспечения безопасности ПДн законных представителей субъектов ПДн, даже если эти лица в локальных актах прямо не упоминаются, но фактически участвуют в правоотношениях с Управлением.

1.1. Основные термины и определения

В настоящем Регламенте применяются термины и определения, установленные Федеральным законом № 152-ФЗ, Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», а также руководящими документами ФСТЭК России, регулирующими вопросы обработки и обеспечения безопасности ПДн.

1.2. Перечень информационных систем, на которые распространяются положения настоящего Регламента

Перечень информационных систем, на которые распространяются положения настоящего Регламента, утверждается приказом начальника Управления в документе «Перечень информационных систем, подлежащих защите в Управлении образования администрации Косинского муниципального округа Пермского края».

1.3. Документы, которыми руководствуется Управление образования администрации Косинского муниципального округа Пермского края при обработке ПДн

Управление при обработке ПДн руководствуется документами, указанными в разделе 6 Политики управления образования администрации Косинского муниципального округа Пермского края в отношении обработки и обеспечения безопасности персональных данных в информационных системах.

Сотрудник Управления, ответственный за обеспечение безопасности информации, в отношении которой установлено требование об обеспечении ее конфиденциальности (далее – Администратор безопасности информации), в своей работе помимо выше перечисленных документов руководствуется следующими локальными актами Управления:

- настоящим Регламентом;

- Политикой управления образования администрации Косинского муниципального округа Пермского края в отношении обработки и обеспечения безопасности персональных данных в информационных системах;

- Инструкцией лица, ответственного за обеспечение безопасности информации, в отношении которой установлено требование об обеспечении ее конфиденциальности, обрабатываемой в информационных системах управления образования администрации Косинского муниципального округа Пермского края ;

- Планом мероприятий по контролю над обеспечением безопасности персональных данных и уровня защищенности информационной системы;

- иными локальными актами Управления в сфере обработки и обеспечения безопасности ПДн.

Сотрудники Управления, непосредственно осуществляющие обработку ПДн, в своей работе помимо выше перечисленных правовых актов руководствуются следующими локальными актами Управления:

- настоящим Регламентом;

- Политикой управления образования администрации Косинского муниципального округа Пермского края в отношении обработки и обеспечения безопасности персональных данных в информационных системах;

- Инструкцией пользователю по соблюдению мер защиты информации, в отношении которой установлено требование об обеспечении ее конфиденциальности;

- Инструкцией по рассмотрению запросов субъектов персональных данных;

- иными локальными актами Управления в сфере обработки и обеспечения безопасности ПДн.

1.4. Принципы обработки ПДн

Обработка ПДн осуществляется в соответствии с принципами, установленными статьей 5 Федерального закона № 152-ФЗ, а также пунктом 7 документа «Политика управления образования администрации Косинского муниципального округа Пермского края в отношении обработки и обеспечения безопасности персональных данных».

Сотрудники Управления, в чьи должностные обязанности входит обработка ПДн, подписывают обязательство о неразглашении информации, в отношении которой

установлено требование об обеспечении ее конфиденциальности, форма которого приведена в приложении 1 к настоящему Регламенту.

1.5. Состав, сроки и цели обработки ПДн

Цели, сроки и состав обрабатываемых персональных данных утверждаются приказом начальника Управления в документе: «Перечень информации, в отношении которой установлено требование об обеспечении ее конфиденциальности (персональных данных), обрабатываемой в информационной системе».

1.6. Способы обработки ПДн

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

Обработка ПДн осуществляется с применением информационных технологий и технических средств в информационных системах. Под техническими средствами, позволяющими осуществлять обработку ПДн, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и прочее), средства обеспечения безопасности ПДн, применяемые в информационных системах.

1.7. Носители ПДн

Носителями ПДн могут являться:

отчуждаемые электронные носители – магнитные и оптические (CD и DVD) накопители, съемные жесткие диски и флэш-накопители, применяемые для получения информации;

неотчуждаемые электронные носители – серверы, ноутбуки, персональные компьютеры и другие электронно-вычислительные машины.

2. Требования к сотрудникам управления образования администрации Косинского муниципального округа Пермского края

Приказом начальника Управления назначается Администратор безопасности информации. Существенным условием является обязанность Администратора безопасности информации обеспечить конфиденциальность ПДн и их безопасность при обработке в информационной системе.

Сотрудники Управления, доступ которых к ПДн, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, допускается к соответствующим ПДн на основании перечня, утверждаемого приказом начальника Управления.

При работе с ПДн в информационной системе сотрудники Управления, допущенные к обработке этих данных в процессе выполнения служебных обязанностей, должны обеспечивать:

- 1) проведение мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и(или) передачи их лицам, не имеющим права доступа к такой информации;
- 2) своевременное обнаружение фактов несанкционированного доступа к ПДн;
- 3) недопущение воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование и целостность данных;
- 4) возможность незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- 5) постоянный контроль за обеспечением уровня защищенности ПДн.

Требования к сотрудникам Управления, работающим с ПДн, включаются в их должностные обязанности в соответствии с Квалификационным справочником должностей руководителей, специалистов и других служащих, утвержденным постановлением Министерства труда и социального развития Российской Федерации от 21 августа 1998 г. № 37.

3. Порядок взаимодействия с субъектами ПДн

Субъект ПДн имеет права на доступ к его ПДн в соответствии со статьей 14 Федерального закона № 152-ФЗ.

Решение, порождающее юридические последствия в отношении субъекта ПДн или иным образом затрагивающее его права и законные интересы на основании исключительно автоматизированной обработки его ПДн не принимается.

Управление разъясняет цели обработки ПДн субъекту ПДн в случае необходимости, а также получает согласие субъекта ПДн на обработку его ПДн в форме, позволяющей подтвердить наличие такого согласия. Форма согласия на обработку и форма разъяснения приведены в приложении 2 и приложении 3, соответственно, к настоящему Регламенту.

Управление рассматривает возражение против автоматизированной обработки в течение тридцати дней со дня его получения и уведомляет субъект ПДн о результатах рассмотрения такого возражения.

4. Реализация Регламента

Управление принимает необходимые и достаточные меры для защиты обрабатываемых ПДн от неправомерного или случайного доступа к ним, от уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий с ними со стороны третьих лиц.

Во исполнение настоящего в Управлении утверждаются следующие локальные акты:

Инструкция пользователю по соблюдению мер защиты информации, в отношении которой установлено требование об обеспечении ее конфиденциальности, в информационных системах Управления образования администрации Косинского муниципального округа Пермского края.

Инструкция лица, ответственного за обеспечение безопасности информации, в отношении которой установлено требование об обеспечении ее конфиденциальности, обрабатываемой в информационных системах Управления образования администрации Косинского муниципального округа Пермского края.

Инструкция по рассмотрению запросов субъектов персональных данных, чьи персональные данные обрабатываются в Управлении образования администрации Косинского муниципального округа Пермского края.

План мероприятий по контролю над обеспечением безопасности персональных данных и уровня защищенности информационной системы.

Ответственный за организацию обработки ПДн в Управлении обязан:

1) осуществлять внутренний контроль за соблюдением в Управлении требований нормативных правовых актов и локальных актов Управления в области обработки и обеспечения безопасности ПДн;

2) доводить до сведения сотрудников Управления положения нормативных правовых актов Российской Федерации и локальных актов Управления в области обработки и обеспечения безопасности ПДн;

3) организовывать прием и обработку обращений и запросов субъектов ПДн или их законных представителей и(или) осуществлять контроль приема и обработки таких обращений и запросов.

В соответствии с требованиями нормативных правовых актов в области обработки и обеспечения безопасности ПДн, обработки ПДн с использованием средств автоматизации в Управлении создаются информационные системы.

При необходимости проводится периодическая классификация информационных систем, определение уровня защищенности, оценка соответствия требованиям по обеспечению безопасности ПДн, оценка эффективности системы защиты информации в соответствии с требованиями нормативных правовых актов в области обеспечения безопасности ПДн.

Для каждой информационной системы:

1) формируется модель угроз безопасности ПДн информационных систем, утверждаемая начальником Управления . На основе модели угроз безопасности ПДн информационных систем проводятся мероприятия по обеспечению безопасности информации в соответствии с требованиями, предъявляемыми к установленному классу (уровню) информационной системы;

2) разрабатывается Описание (Технический паспорт) информационной системы, утверждаемое начальником Управления;

3) разрабатывается Технологический процесс обработки информации в информационной системе, утверждаемый начальником Управления;

4) разрабатывается Перечень информации, в отношении которой установлено требование об обеспечении её конфиденциальности, обрабатываемой в информационной системе;

5) разрабатывается Перечень защищаемых ресурсов конфиденциального характера и матрица доступа субъектов информационной системы к защищаемым информационным ресурсам.

Пересмотр моделей угроз для каждой информационной системы осуществляется:

1) в плановом порядке для существующих информационных систем – ежегодно;

2) в случае существенных изменений в инфраструктуре информационной системы или порядке обработки ПДн в информационной системе – в течение трех месяцев с даты фиксации изменений;

3) в случае создания новой информационной системы (выделения части из существующей информационной системы) – в течение одного месяца с даты создания (выделения) информационной системы.

В Управлении запрещается обработка ПДн в целях, не соответствующих целям создания информационной системы, эксплуатация информационной системы в составе, отличном от указанного при создании информационной системы.

В целях обеспечения управления информационной безопасностью ПДн в Управлении создается система защиты ПДн (далее – СЗПДн).

Объектами защиты СЗПДн являются информация, обрабатываемая Управлением и содержащая ПДн, а также инфраструктура, содержащая и поддерживающая указанную информацию.

СЗПДн реализуется комплексом правовых, организационных и технических мер, которые включают:

1) подготовку локальных актов Управления по вопросам обработки и обеспечения безопасности ПДн, контроль за исполнением в Управлении требований нормативных правовых актов и локальных актов Управления в области обработки и обеспечения безопасности ПДн, а также внесение соответствующих изменений в имеющиеся локальные акты Управления;

2) письменное оформление обязательств сотрудников Управления о неразглашении ПДн;

3) доведение до сведения сотрудников Управления информации об установленной законодательством Российской Федерации ответственности за нарушения, связанные с обработкой и обеспечением безопасности ПДн;

4) обеспечение наличия в положениях о структурных подразделениях Управления и должностных обязанностях требований по соблюдению установленного порядка обработки и обеспечения безопасности ПДн;

5) разработку и введение в действие локальных актов Управления по обеспечению безопасности информационной системы;

6) регламентацию процедур создания и осуществление документирования действующих инженерных и информационных систем, программных комплексов, порядка внесения в них изменений и своевременной актуализации эксплуатационной документации;

7) ознакомление сотрудников Управления с положениями нормативных правовых актов Российской Федерации и локальных актов в области обработки и обеспечения безопасности ПДн и(или) организацию обучения их правилам обработки и обеспечения безопасности ПДн;

8) проведение мероприятий в форме утверждения планов проверки и контроля по регламентации, установлению, поддержанию и осуществлению контроля за состоянием:

8.1) контрольно-пропускного режима, а также за перемещением технических средств и машинных носителей информации;

8.2) защиты технологических процессов, информационных ресурсов, информации и поддерживающей их инфраструктуры от угроз техногенного характера и внешних неинформационных воздействий;

9) регламентацию в форме инструкций сотрудникам Управления, участвующим в обработке ПДн, а также отвечающим за организацию обработки и обеспечение безопасности ПДн правил обработки ПДн, в том числе хранение и передачу информации внутри Управления при взаимодействии с контрагентами Управления, государственными органами и организациями, обращения с документами (включая электронные документы) и машинными носителями, порядка их учета, хранения и уничтожения;

10) установление в форме инструкций и перечней сотрудникам Управления правил доступа на объекты, в помещения, в информационную систему, применения в этих целях систем охраны и управления доступом;

11) формирование участков (например, выделение в отдельные виртуальные локальные компьютерные сети технических средств) администрирования безопасности, мониторинга и аудита, управление доступом к защищаемым ресурсам;

12) организацию технического оснащения объектов и информационной системы в соответствии с существующими требованиями к информационной безопасности;

13) формирование условий и технологических процессов обработки, хранения и передачи информации в Управлении (включая условия хранения документов в архивах), обеспечивающих реализацию требований нормативных правовых актов, методических документов уполномоченных государственных органов и локальных актов Управления в области обработки и обеспечения безопасности ПДн;

14) установление полномочий пользователей и форм представления информации пользователям информационной системы;

15) организацию непрерывного процесса контроля (мониторинга) событий безопасности для своевременного выявления и пресечения попыток несанкционированного доступа к ПДн;

16) организацию необходимых мероприятий с сотрудниками Управления, а также собеседование с лицами, претендующими на работу в Управлении, изучение их биографии и проверку предоставляемых сведений; обучение сотрудников Управления требованиям информационной безопасности;

17) осуществление контроля эффективности организационных мер защиты;

18) разработку защитных технических решений:

18.1) при стратегическом планировании архитектуры информационной системы;

18.2) при выборе технических средств обработки информации;

18.3) при разработке и(или) приобретении программного обеспечения;

19) применение следующих компонентов технических мер защиты:

19.1) защищенных средств (систем) обработки информации, содержащей ПДн;

19.2) межсетевых экранов для логического разделения подсетей и защиты от несанкционированного доступа из внешних (открытых) информационных систем;

19.3) аппаратных и программных средств защиты и контроля, устройств, технических систем и средств, используемых для обеспечения информационной безопасности, в том числе для обнаружения и нейтрализации попыток несанкционированного доступа к информации.

Сотрудники Управления ознакамливаются с локальными актами управления, регламентирующими необходимые действия по обеспечению целостности и доступности ПДн в нештатных ситуациях.

По окончанию сроков обработки ПДн создается комиссия, утверждаемая приказом заведующего Управления, из сотрудников Управления для уничтожения ПДн. Данные ПДн комиссионно уничтожаются и составляется акт об уничтожении, форма которого приведена в приложении 4 к настоящему Регламенту.

5. Правила допуска, хранения и пересылки ПДн

Допуск сотрудников Управления к обработке ПДн в информационной системе осуществляется на основании соответствующих разрешительных документов и ключей (паролей) доступа.

Пересылка ПДн без использования специальных средств защиты информации по общедоступным сетям связи, в том числе сети «Интернет», запрещается.

Пересылка ПДн разрешается только в соответствии с целями обработки ПДн по каналам связи, расположенным в пределах контролируемой зоны, либо по защищенным каналам связи с помощью средств защиты информации, прошедших оценку соответствия в ФСБ России и/или ФСТЭК России.

6. Ответственность за нарушение норм, регулирующих обработку ПДн

Сотрудники Управления, виновные в нарушении норм, регулирующих обработку и обеспечение безопасности ПДн, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

7. Заключительные положения

Настоящий Регламент вступает в силу с момента ввода в действие приказом начальника Управления.

Настоящий Регламент доводится до сведения всех сотрудников Управления персонально под подпись, а также до сотрудников, вновь принимаемых на работу.

Приложение 1
к Регламенту управления образования
администрации Косинского муниципального
округа Пермского края в отношении
обработки и обеспечения безопасности
персональных данных

Форма

ОБЯЗАТЕЛЬСТВО

о неразглашении информации, в отношении которой установлено требование об обеспечении ее конфиденциальности

Я,

(фамилия, имя, отчество, адрес, документ, удостоверяющий личность)

сотрудник Управления образования администрации Косинского муниципального округа Пермского края, обязуюсь:

не разглашать персональные данные физических лиц и другую информацию, в отношении которой установлено требование об обеспечении ее конфиденциальности (далее – сведения ограниченного доступа), которые будут доверены мне Управлением образования администрации Косинского муниципального округа Пермского края или станут известны в период действия служебного контракта, а также сведения ограниченного доступа сторонних предприятий и организаций, переданные мне в ходе служебной деятельности;

не сообщать устно или письменно кому бы то ни было сведения ограниченного доступа без соответствующего разрешения имеющих на то право лиц;

в случае попытки посторонних лиц получить сведения ограниченного доступа немедленно сообщать об этом своему непосредственному руководителю;

не использовать знание сведений ограниченного доступа для занятий любой деятельностью, которая в качестве конкурентного действия может нанести ущерб Управлению образования администрации Косинского муниципального округа Пермского края;

при прекращении действия служебного контракта все машинные носители сведений ограниченного доступа (документы, электронные носители, черновики, распечатки на принтерах и пр.), которые находились в моем распоряжении в связи с выполнением должностных обязанностей, передать своему непосредственному руководителю;

об утрате или недостаче машинных носителей сведений ограниченного доступа, удостоверений, пропусков, ключей от сейфов (хранилищ), личных печатей и других фактах, которые могут привести к разглашению сведений ограниченного доступа, а также о причинах и условиях возможной утечки этих сведений немедленно сообщать непосредственному руководителю;

использовать переданные мне Управлением образования администрации Косинского муниципального округа Пермского края и установленные на рабочем месте технические средства обработки и передачи информации исключительно для выполнения обязанностей, предусмотренных служебным контрактом.

Управление образования администрации Косинского муниципального округа Пермского края предоставило мне необходимые условия для выполнения требований по охране сведений ограниченного доступа, к которым я допущен: хранилища для документов, средства для доступа к информационным ресурсам (ключи, пароли и т.п.) и др., определяемые обязанностями, выполняемыми мною.

Управление образования администрации Косинского муниципального округа Пермского края оставляет за собой право, но не принимает каких-либо обязательств контролировать надлежащее использование мною технических средств обработки и хранения информации, соблюдение мною мер по защите персональных данных.

Я предупрежден, что разглашение сведений ограниченного доступа, ставших мне известными в период действия служебного контракта, может повлечь дисциплинарную, материальную, административную, гражданско-правовую, уголовную ответственность, предусмотренную действующим законодательством Российской Федерации.

«____» 20 __г.

(подпись)

Проинструктировал:

«____» 20 __г.

(подпись)

Приложение 2
к Регламенту управления образования
 администрации Косинского муниципального
 округа Пермского края в отношении
 обработки и обеспечения безопасности
 персональных данных

СОГЛАСИЕ

работника Управления образования администрации Косинского муниципального округа Пермского края на обработку персональных данных

Я,

(Ф.И.О. полностью)

зарегистрированный (-ая) по адресу:

(индекс и адрес регистрации согласно паспорта)

паспорт серия _____ № _____ выдан _____

(орган, выдавший паспорт и дата выдачи)

являясь работником Управления образования администрации Косинского МО ПК
находящегося по адресу: 619430 с.Коса ул.Ленина,66

в соответствии со ст. 9 Федерального закона от 27.07.2006г. № 152-ФЗ «О защите
персональных данных» даю согласие на обработку своих персональных данных, а именно:
совершение действий, предусмотренных п. 3 ст. 3 Федерального закона № 152-ФЗ со всеми
данными, которые находятся в распоряжении Управления образования администрации
Косинского МО ПК с целью начисления заработной платы, исчисления и уплаты
предусмотренных законодательством РФ налогов, сборов и взносов на обязательное
социальное и пенсионное страхование, представления организацией-работодателем
установленной законодательством отчетности в отношении физических лиц, в том числе
сведений персонализированного учета в Пенсионный фонд РФ, сведений подоходного
налога в ФНС РФ, сведений в ФСС РФ, предоставлять сведения в банк для оформления
банковской карты и перечисления заработной платы на карты, и третьим лицам для
оформления полиса ОМС, а также предоставлять сведения в случаях, предусмотренных
федеральными законами и иными нормативно-правовыми актами, следующих моих
персональных данных:

Перечень персональных данных, на обработку которых дается согласие:

фамилия, имя, отчество (в т.ч. предыдущие),

паспортные данные или данные документа, удостоверяющего личность,

дата рождения, место рождения,

гражданство,

отношение к воинской обязанности и иные сведения военного билета и приписного
удостоверения,

данные документов о профессиональном образовании, профессиональной переподготовки,
повышении квалификации, стажировке,

данные документов о подтверждении специальных знаний,

данные документов о присвоении ученой степени, ученого звания, списки научных трудов и
изобретений и сведения о наградах и званиях,

знание иностранных языков,

семейное положение и данные о составе и членах семьи,

сведения о социальных льготах, пенсионном обеспечении и страховании,

данные документов об инвалидности (при наличии),
данные медицинского заключения (при необходимости),
стаж работы и другие данные трудовой книжки и вкладыша к трудовой книжке,
должность, квалификационный уровень,
сведения о заработной плате (доходах), банковских счетах, картах,
адрес места жительства (по регистрации и фактический), дата регистрации по указанному
месту жительства,
номер телефона (рабочий, домашний, мобильный),
данные свидетельства о постановке на учет в налоговом органе физического лица по месту
жительства на территории РФ (ИНН),
данные страхового свидетельства государственного пенсионного страхования,
данные страхового медицинского полиса обязательного страхования граждан.

- в целях информационного обеспечения для формирования общедоступных источников персональных данных (информации на официальном сайте Управления образования) и других документов на обработку следующих персональных данных: *фамилия, имя и отчество; дата рождения; номера рабочих и сотовых телефонов; адрес электронной почты; сведения о должности; фотографии на бумажном носителе и в электронной форме; иные данные, предоставленные мной для размещения в общедоступных источниках персональных данных.*

Перечень действий, на совершение которых дается согласие:

Разрешаю Оператору (организации-работодателю) производить с моими персональными данными действия (операции), определенные статьей 3 Федерального закона от 27.07.2006 №152-ФЗ, а именно: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Обработка персональных данных может осуществляться как с использованием средств автоматизации, так и без их использования (на бумажных носителях).

Согласие на передачу персональных данных третьим лицам:

Разрешаю обмен (прием, передачу, обработку) моих персональными данных между Оператором (организацией-работодателем) и третьими лицами в соответствии с заключенными договорами и соглашениями, в целях соблюдения моих законных прав и интересов.

Я ознакомлен(а), что:

1) согласие на обработку персональных данных действует с даты подписания настоящего согласия в течение всего срока работы в Управлении образования администрации Косинского МО ПК;

2) согласие на обработку персональных данных может быть отозвано на основании письменного заявления в произвольной форме;

3) в случае отзыва согласия на обработку персональных данных, Управление образования администрации Косинского МО ПК вправе продолжить обработку персональных данных без согласия при наличии оснований, указанных в пунктах 2-11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных";

4) после прекращения трудовых отношений персональные данные хранятся в Управлении образования администрации Косинского МО ПК в течение срока хранения документов, предусмотренных действующим законодательством Российской Федерации;

5) персональные данные, предоставляемые в отношении третьих лиц, будут обрабатываться только в целях осуществления и выполнения возложенных законодательством Российской Федерации на Управление образования администрации Косинского МО ПК функций, полномочий и обязанностей.

Дата начала обработки персональных данных:

(число, месяц, год)

(подпись)

Приложение 3
к Регламенту управления образования
администрации Косинского муниципального
округа Пермского края в отношении
обработки и обеспечения безопасности
персональных данных

**Типовая форма
разъяснения субъекту персональных данных юридических последствий отказа
предоставить свои персональные данные управлению образования администрации
Косинского муниципального округа Пермского края с целью**

Мне, _____,
разъяснены юридические последствия отказа предоставить свои персональные данные в
управление образования администрации Косинского муниципального округа Пермского
края.

Управление образования администрации Косинского муниципального округа
Пермского края осуществляет обработку персональных данных на основе законодательства
Российской Федерации, регламентирующего правила обработки персональных данных, а
также на основе принятой в Управлении образования администрации Косинского
муниципального округа Пермского края Политики управления образования администрации
Косинского муниципального округа Пермского края в отношении обработки и обеспечения
безопасности персональных данных.

Обработка персональных данных в Управлении образования администрации
Косинского муниципального округа Пермского края осуществляется в связи с выполнением
Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Мне как субъекту персональных данных разъяснено,
что без предоставления данных, обязательных для _____,
_____, мне будет отказано в
_____.

«___» ____ 20 ____ г. /_____
(дата) (Подпись) /_____
(Расшифровка подписи)

Разъяснение провел /_____
(Подпись) /_____
(Расшифровка подписи)

Приложение 4
к Регламенту управления образования
администрации Косинского муниципального
округа Пермского края в отношении
обработки и обеспечения безопасности
персональных данных

Форма

**АКТ №
уничтожения персональных данных,
находящихся в информационной системе**

(Место уничтожения)

« _____ » 20 ____ г.
(Дата уничтожения)

Комиссия в составе:

Председатель комиссии:

(Должность)

(ФИО)

Члены комиссии:

(Должность)

(ФИО)

(Должность)

(ФИО)

(Должность)

(ФИО)

(Должность)

(ФИО)

составили настоящий акт о том, что « _____ » 20 ____ г. произведено
уничтожение персональных данных, находящихся на:

(наименование АРМ по утвержденной конфигурации, ФИО ответственного пользователя
АРМ, заводской или учетный номер системного блока ПЭВМ, носителя информации, способ
уничтожения информации)

Уничтожены персональные данные в соответствии с таблицей:

Подписи членов комиссии:

Председатель комиссии:

Члены комиссии:

_____ (Подпись) _____ (ФИО) _____ « » 20 г.
_____ (Дата)

_____ (Подпись) _____ (ФИО) _____ « » 20 г.
_____ (Дата)

_____ / _____ / « _____ » 20 г.
(Подпись) (ФИО) (Дата)

_____ / _____ / _____
(Подпись) (ФИО) « _____. _____. _____. г.
_____ / _____ / _____
(Дата)