

**ИНСТРУКЦИЯ**  
**пользователя по работе с персональными данными в ГИС**  
**«Электронное образование»**

**1. Общие положения**

1.1. Настоящая Инструкция определяет общие правила работы сотрудников образовательных организаций и Управления образования МР «Корткеросский» (далее – Образование) с персональными данными в ГИС «Электронное образование».

1.2. Персональные данные в электронном виде обрабатываются в информационных системах персональных данных. Также устанавливается особый порядок обработки и хранения персональных данных, содержащихся на бумажных носителях.

1.3. Пользователем является каждый сотрудник Образования, участвующий в рамках своих функциональных обязанностей в процессах, как автоматизированной обработки, так и обработки без использования средств автоматизации персональных данных, а также имеющий доступ к аппаратным средствам, программному обеспечению, носителям информации и средствам защиты.

1.4. Пользователь в своей работе руководствуется настоящей Инструкцией, Правилами обработки персональных данных, руководящими и нормативными документами ФСТЭК России и ФСБ России и другими документами Образования, регламентирующими обработку персональных данных.

1.5. Методическое руководство по работе Пользователя осуществляет ответственный за организацию обработки персональных данных.

**2. Термины и определения**

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

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

предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

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

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

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

2.6. Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.7. Автоматизированное рабочее место (АРМ) – программно-технический комплекс, посредством которого Пользователь выполняет свои должностные обязанности (персональный компьютер, ноутбук, терминал и т.п.).

2.8. Несанкционированный доступ (НСД) – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

2.9. Посторонние лица – лица, которые не имеют права самостоятельного доступа в помещение и (или) не имеют права самостоятельного доступа в ИСПДн и (или) не имеют допуска к персональным данным.

2.10. Средство защиты информации от несанкционированного доступа (СЗИ от НСД) – программное, техническое или программно-техническое средство, направленное на предотвращение или существенное затруднение несанкционированного доступа к информации.

### **3. Обязанности пользователя**

3.1. Не разглашать персональные данные, которые будут доверены или станут известны в ходе рабочего процесса во время выполнения должностных (договорных) обязанностей.

3.2. Не сообщать устно или письменно, не передавать в каком-либо виде третьим лицам и не раскрывать публично персональные данные без соответствующего разрешения **руководителя**.

3.3. Знать и выполнять требования законодательных актов Российской Федерации, настоящей Инструкции и других внутренних документов, регламентирующих порядок обработки персональных данных.

**3.4.** Выполнять на АРМ только те процедуры обработки персональных данных, которые определены должностной инструкцией.

**3.5.** Знать и соблюдать установленные требования обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности персональных данных.

**3.6.** Использовать для хранения персональных данных только определенные места хранения и учтенные носители персональных данных.

**3.7.** Незамедлительно, в кратчайшие сроки, сообщать руководителю об утрате или недостатке носителей информации, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов и о других фактах, которые могут привести к разглашению персональных данных.

**3.8.** При прекращении работ (трудовых отношений) все материальные носители, содержащие персональные данные (флеш-накопители, дискеты, оптические диски, документы, черновики, распечатки на принтерах, кино- и фотоматериалы, модели, промышленные образцы и пр.), передать **руководителю**.

**3.9.** Соблюдать требования парольной политики (раздел 4).

**3.10.** Соблюдать требования антивирусной защиты (раздел 5).

**3.11.** Пользователи, имеющие выход в Интернет, обязаны соблюдать правила при работе в сетях связи общего пользования и (или) сетях международного информационного обмена (раздел 6).

**3.12.** Пользователи, работающие с электронной подписью или использующие шифрование, обязаны соблюдать Инструкцию по обращению со средствами криптографической защиты информации.

**3.13.** Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

**3.14.** Обо всех выявленных нарушениях, связанных с порядком обработки персональных данных, а также для получения консультаций по вопросам обработки персональных данных, необходимо обращаться к ответственному за организацию обработки персональных данных.

**Пользователям запрещается:**

**3.14.1.** Нарушать установленные в Образовании инструкции по работе с персональных данных.

**3.14.2.** Использовать компоненты программного и аппаратного обеспечения Образования в неслужебных целях.

**3.14.3.** Оставлять свое рабочее место без присмотра, предварительно не заблокировав (штатными средствами операционной системы Windows – комбинацией клавиш [WIN] + [L] или [CTRL] + [ALT] + [DEL] с дальнейшим нажатием кнопки «Блокировка» появившегося меню, либо при помощи штатных средств защиты

информации от несанкционированного доступа при их наличии).

**3.14.4.** Оставлять без присмотра или неубранными в хранилища (шкаф, сейф) носители или документы, содержащие персональные данные.

**3.14.5.** Записывать и хранить персональные данные на неучтенных носителях информации (оптических дисках, гибких магнитных дисках, флеш-накопителях и т.п.).

**3.14.6.** Самовольно изменять состав и конфигурацию используемых программных, аппаратных, программно-аппаратных средств, самовольно устанавливать программное обеспечение, отключать/подключать оборудование или изменять режимы его работы.

**3.14.7.** Самовольно подключать АРМ или другие средства к ЛВС ГАУ РК «ЦИТ», изменять IP-адрес, MAC-адрес и иные настройки сети АРМ.

**3.14.8.** Производить действия, направленные на получение несанкционированного доступа к АРМ и серверам, равно как и любым другим узлам ЛВС Образования или Интернет, в том числе:

- действия, направленные на нарушение нормального функционирования элементов сети (компьютеров, другого сетевого оборудования или программного обеспечения);

- установка программного обеспечения, осуществляющего перехват информации (информационных пакетов), адресованной другим пользователям;

- действия, направленные на получение несанкционированного доступа к информационным ресурсам, в последующем использовании такого доступа;

- уничтожение, модификация программного обеспечения или данных без согласования с **руководителем** или владельцами этого ресурса;

- попытки подбора паролей к любым информационным ресурсам методом перебора всех возможных вариантов паролей, либо атак по словарю;

- умышленные действия по созданию, использованию и распространению вредоносных программ, в том числе направленных на получение несанкционированного доступа к любым информационным и служебным ресурсам (как внутри Образования, так и вне), либо на нарушение целостности и работоспособности этих систем;

- действия по сканированию локальной сети с целью определения ее внутренней структуры, списков открытых портов, наличия существующих сервисов и уязвимостей.

**3.14.9.** Самовольно изменять параметры средств защиты информации (в том числе и средств антивирусной защиты), а также завершать их работу и (или) самостоятельно их устанавливать.

Самостоятельно разрабатывать или использовать нерегламентированные (без разрешения **руководителя**, не относящиеся

к производственному процессу) программы (например: игры; IM-клиенты, такие как Google Messenger, ICQ и т.п.; P2P-клиенты: Kazaa, eMule и т.п.).

**3.14.10.** Разрешать посторонним лицам работать под своей учетной записью в ИСПДн.

**3.14.11.** Пересылать персональные данные по каналам связи в открытом виде, в том числе Интернет, по телефону, факсу, электронной почте и т.п. (без использования средств шифрования).

**3.14.12.** Получать доступ к персональным данным с рабочих мест, не оборудованными необходимыми средствами защиты информации.

**3.14.13.** Самовольно создавать совместно используемые сетевые ресурсы (папки общего доступа) на своих компьютерах и файловых серверах, несанкционированно удалять или изменять права доступа к ним.

**3.14.14.** В случае возникновения любых механических неисправностей в оборудовании осуществлять самостоятельные попытки их устранения.

**3.14.15.** Препятствовать должностным лицам при проведении проверок и служебных расследований, связанных с обеспечением безопасности информации.

**3.14.16.** Удалять или искажать программы и файлы с персональными данными и иной важной информацией (например, системной, необходимой для функционирования ИСПДн).

**3.14.17.** Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению внештатной ситуации. Об обнаружении такого рода ошибок – ставить в известность руководителя своего подразделения и сотрудников, ответственных за установку и (или) сопровождение программного обеспечения (Администратора безопасности персональных данных в информационных системах персональных данных (далее - администратор безопасности)).

**3.14.18.** Подключать к ЛВС Образования личные средства вычислительной техники: ноутбуки, карманные компьютеры, смартфоны и т.п., а также личные носители и накопители информации. В случае необходимости переноса информации с личных носителей информации обращаться к ответственным.

## **4. Парольная политика**

### **4.1. Общие требования к паролям:**

- Минимальное требование: буквенно-цифровой пароль. Желательно использовать буквы в верхнем или нижнем регистрах, цифры или специальные символы (например: ~ ! @ # \$ % ^ & \* ( ) \_ - + =

| \ ? / . , ; ' ] [ { } < > . и т.п.).

- Минимальная длина пароля: не менее 6 (шести) символов.
- Максимальный срок действия пароля: 90 суток.
- Запрет использования трех ранее использовавшихся паролей.

- Пароль Пользователя не должен включать в себя легко вычисляемые сочетания символов, общепринятые сокращения, имена, фамилии, должности, год рождения, номер паспорта, табельный номер, иную информацию о Пользователе, доступную другим лицам.

- Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов.

- Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например: 1234567, qwerty и т.п.).

#### **4.2. Правила использования паролей:**

- Хранить в тайне свой пароль, не сообщать его другим лицам.
- Не предоставлять доступ в ИСПДн другим лицам под своей учетной записью и паролем.

- Изменять свой пароль при первом требовании политики паролей операционной системы и/или ИСПДн.

- Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

- Запрещается записывать свои пароли в очевидных местах, внутри ящика стола, на мониторе АРМ, на обратной стороне клавиатуры и т.д.

- Запрещается хранить пароли в записанном виде на отдельных листах бумаги.

#### **4.3. Смена, удаление личного пароля любого Пользователя производится в следующих случаях:**

- в случае подозрения на компрометацию пароля;
- по окончании срока действия;
- в случае прекращения полномочий (увольнение, переход на другую работу внутри Образования) Пользователя после окончания последнего сеанса работы в информационных системах персональных данных;

- по указанию ответственного за организацию обработки персональных данных.

**4.4.** При увольнении, переходе на новую должность сотрудника, имеющего доступ помимо своей учетной записи к другим ресурсам (межсетевые экраны, маршрутизаторы, серверы, другие учетные записи и т.п.) также производится внеплановая смена паролей к таким ресурсам.

## **5. Применение личных идентификаторов в информационной системе персональных данных**

Привязку идентификатора к пользователю (учетной записи) выполняет администратор безопасности.

5.1. Пользователи ИСПДн получают свой идентификатор у администратора безопасности.

5.2. Пользователь ИСПДн обязан хранить свой личный идентификатор в недоступных для других сотрудников хранилищах.

5.3. Пользователю ИСПДн запрещается передавать свой личный идентификатор.

5.4. В случае утери личного идентификатора, пользователь ИСПДн должен немедленно доложить об этом администратору безопасности информации.

5.5. В случае прекращения полномочий учетной записи пользователя ИСПДн (увольнение, переход на другую работу, в другой отдел или помещение, а также другие обстоятельства) учетная запись должна быть удалена, а её идентификатор должен быть сдан администратору безопасности информации после окончания последнего сеанса работы данного пользователя в ИСПДн.

5.6. В случае компрометации или утери личного идентификатора пользователя администратором безопасности должны быть немедленно предприняты меры в соответствии с п. 5.7 настоящей Инструкции.

5.7. Администратор безопасности информации должен провести служебное расследование для выяснения причин компрометации идентификатора с целью выработки новых или совершенствования принятых технических и организационных мер по устранению такой угрозы в будущем, а также выяснению величины ущерба, который может быть нанесен собственнику информационных ресурсов.

## **6. Антивирусная защита**

6.1. В случае отсутствия штатных функций антивирусной программы, предусматривающих автоматическую проверку файлов, Пользователь обязан осуществлять проверку файлов получаемых:

- по электронной почте;
- через сеть Интернет;
- на магнитном, оптическом диске, флеш-накопителе;
- ином съемном носителе информации;
- полученные иным способом.

6.2. Перед открытием вложения (ссылок) убедиться в том, что отправитель действительно послал вам этот файл, даже если он и должен был это сделать. Позвоните ему сами. Не доверяйте имени отправителя и указанным в тексте письма номерам телефонов, а также лицам, позвонившим вам самостоятельно с просьбой открыть файлы и

пройти по ссылкам.

### **6.3. Пользователю запрещается:**

**6.3.1.** Осуществлять действия, направленные на выключение антивирусной программы.

**6.3.2.** Самостоятельно устанавливать на АРМ программное обеспечение.

**6.3.3.** Запускать файлы, полученные по сетям связи (электронной почте, Интернет), со съемных носителей, даже если они получены проверенного адресата, без предварительной их проверки антивирусной программой.

**6.3.4.** При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) Пользователь самостоятельно или вместе с ответственным (Администратором безопасности) должен провести внеочередной антивирусный контроль своего рабочего места.

**6.3.5.** В случае обнаружения при проведении антивирусной проверки вирусного заражения Пользователи обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения вирусного заражения ответственному (Администратору безопасности);
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов.

## **7. Порядок работы в ИСПДн и сети интернет**

### **7.1. Подключение к ИСПДн и сети Интернет**

**7.2.** Целью работы Пользователя в ИСПДн и сети Интернет является сбор, обработка, хранение персональных данных, обмен электронными сообщениями в служебных целях.

**7.2.1.** Доступ к ИСПДн и сети Интернет предоставляется Пользователям только в том случае, если это не противоречит требованиям настоящей Инструкции и иными нормативными документами в области защиты информации.

**7.2.2.** Доступ пользователя к ИСПДн для обработки персональных данных производится только с рабочих мест, на которых установлены средства защиты информации.

**7.2.3.** Основанием для подключения сотрудника Образования к ИСПДн и сети Интернет является мотивированная заявка ответственному за организацию обработки персональных данных от непосредственного руководителя Пользователя с указанием полномочий доступа к таким ресурсам и сервисам.

**7.2.4.** Ответственный за организацию обработки персональных



данных, либо сотрудник, выполняющий его функции, организует подключение к ИСПДн или сети Интернет Пользователей в установленном порядке, осуществляет контроль над использованием данных ресурсов и сервисов.

**7.2.5.** После выполнения задания Ответственный за организацию обработки персональных данных сообщает пользователю выполнении заявки.

**7.2.6.** Основанием для отключения пользователя от ИСПДн и сети Интернет являются следующие события:

- нарушение инструкций и иных локальных нормативных актов в области защиты информации;
- увольнение Пользователя, либо перевод его в другое подразделение.

### **7.3. Порядок работы в сети Интернет**

**7.3.1.** Использование сотрудниками Образования сети Интернет должно осуществляться исключительно для выполнения должностных обязанностей.

**7.3.2.** Информация, образованная (образующаяся) в процессе трудовой деятельности работника Образования является собственностью Образования и не подлежит использованию (в том числе использованию в сети Интернет или с помощью сети Интернет) в личных целях и (или) в корыстных интересах других лиц (организаций).

**7.3.3.** При проведении технических работ, связанных с настройкой оборудования (коммуникационное оборудование, прокси-сервера, маршрутизаторы и т.п.); в случае обнаружения попыток несанкционированного доступа к Интернет-шлюзу, АРМ Пользователей может проводиться временное отключение Пользователей от сервисов сети Интернет (в случае планового отключения Пользователи уведомляются об этом заблаговременно).

**7.3.4.** Вся информация о ресурсах, посещаемых сотрудниками Образования, протоколируется и, при необходимости, может быть предоставлена руководителям подразделений, а также руководству Образования для детального изучения и принятия решения о мерах дисциплинарной ответственности.

**7.3.5.** При работе в сети Интернет Пользователям запрещается:

- умышленное распространение и получение материалов в/из сети Интернет, противоречащих законодательству Российской Федерации, в том числе материалов, пропагандирующих насилие или экстремизм; разжигающих расовую, национальную или религиозную вражду; разъясняющих порядок изготовления и/или применения наркотиков, взрывчатых веществ, оружия и т. п.; материалов порнографического характера; компьютерных вирусов и других вредоносных программ;

- передавать в сеть Интернет информацию, к которой в соответствии с законодательством ограничен доступ (персональные данные, служебная информация) без соответствующего разрешения;
- фальсифицировать IP-адрес, MAC-адрес, иные адреса, используемые в сетевых протоколах, а также прочую информацию при передаче данных через сеть Интернет.
- предоставлять доступ в сеть Интернет со своей рабочей станции кому-либо, в том числе программно-техническими способами через локальную вычислительную сеть Образования (например: путем несанкционированной установки локального Интернет-шлюза на рабочее место);
- получать доступ к сети Интернет любыми способами, не предусмотренными действующими локальными документами (Инструкциями, Правилами, Регламентами Образования);
- осуществлять несанкционированный доступ к ресурсам и сервисам сети Интернет.
- выполнять действия (взлом, DoS (отказ в обслуживании), ARP-spoofing атаки, сканирование локальной вычислительной сети) направленные на нарушение функционирования элементов сети Интернет (коммуникационного оборудования, серверов, рабочих станций, программного обеспечения).

#### **7.4. Правила работы Пользователей с электронной почтой:**

**7.4.1.** Пользователи обязаны использовать электронную почту только для выполнения служебных обязанностей.

**7.4.2.** Запрещается отправлять файлы, содержащие персональные данные в открытом виде (не зашифрованные).

**7.4.3.** Запрещается массовая рассылка почтовых сообщений (более 100) внешним адресатам без согласования с руководством (спама).

**7.4.4.** Запрещается использовать не свой обратный адрес при отправке электронной почты.

**7.4.5.** Запрещается отправлять по электронной почте исполняемые файлы (обычно имеют расширения exe, com, bat, js, vbs и т.п.). В случае необходимости отправки таких файлов, помещать их в архив и установить пароль.

**7.4.6.** Присоединяемые файлы рекомендуется упаковывать в архив при помощи программ-архиваторов.

**7.4.7.** Корпоративные рекомендации использования электронной почты:

- Вы должны оказывать то же уважение, что и при устном общении.
- Вы должны проверять правописание, грамматику и дважды перечитывать свое сообщение перед отправлением.
- Вы не должны участвовать в рассылке посланий, пересылаемых по цепочке (чаще всего это письма религиозно-мистического, развлекательного содержания).

- Вы не должны по собственной инициативе пересылать по произвольным адресам незатребованную информацию.
- Вы не должны рассылать сообщения, которые являются зловредными, раздражающими или содержащими угрозы другим пользователям.
- Вы не должны отправлять никаких сообщений противозаконного или неэтичного содержания.
- Вы должны помнить, что электронное послание является эквивалентом почтовой открытки и не должно использоваться для пересылки персональных данных без использования средств защиты (шифрование).
- Вы не должны использовать широковещательные возможности электронной почты за исключением выпуска уместных объявлений.
- Вы не должны использовать корпоративную электронную почту для посланий личного характера.
- Вы должны неукоснительно соблюдать правила и инструкции и помогать администраторам бороться с нарушителями правил.

## **8. Порядок работы со съемными носителями информации**

**8.1.** Под использованием носителей информации в ИСПДн Образования понимается их подключение к инфраструктуре ИСПДн с целью обработки, приема/передачи информации между информационными системами и носителями информации.

**8.2.** Допускается использование только учтенных носителей информации, которые являются собственностью Образования и подвергаются регулярной ревизии и контролю.

**8.3.** Учет и выдачу съемных носителей информации осуществляет лицо, ответственное за организацию обработки персональных данных. Факт выдачи носителя фиксируется в журнале учета машинных носителей информации.

**8.4.** Если доступ к ИСПДн производится при помощи персональных идентификаторов (eToken, Rutoken, др.), то факт получения и сдачи данных идентификаторов обязательно фиксируется ответственным за организацию обработки персональных данных, в соответствующих журналах.

**8.5.** Возможность подключения носителей информации, а также получение учтенных носителей информации предоставляются Пользователям по инициативе руководителей структурных подразделений в случаях:

- необходимости выполнения вновь принятым работником своих должностных обязанностей;
- возникновения у Пользователя служебной необходимости.

**8.6.** При использовании носителей информации необходимо:

- использовать носители информации исключительно для выполнения своих служебных обязанностей;
- бережно относиться к носителям персональных данных.
- обеспечивать физическую безопасность носителей информации всеми разумными способами;
- извещать ответственного за организацию обработки персональных данных о фактах утраты (кражи) носителей информации.

**8.7.** При использовании носителей персональных данных запрещено:

- использовать носители персональных данных в личных целях;
- передавать носители персональных данных другим лицам (за исключением администраторов);
- хранить съемные носители с персональными данными на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;
- выносить съемные носители с персональными данными из служебных помещений для работы с ними на дому и т. д.

**8.8.** Любое взаимодействие (обработка, прием/передача информации) инициированное Пользователем между информационной системой и неучтенными (личными) носителями информации, рассматривается как несанкционированное (за исключением случаев оговоренных с администраторами заранее). Ответственный за организацию обработки персональных данных с привлечением помощи (если необходимо) сотрудников ГБУ Республики Коми «ЦБИ» на основании Соглашения оставляет за собой право блокировать или ограничивать использование носителей информации.

**8.9.** Информация об использовании Пользователями носителей информации в информационных системах протоколируется и, при необходимости, может быть предоставлена руководителям структурных подразделений, а также руководителю.

**8.10.** В случае выявления фактов несанкционированного и/или нецелевого использования носителей информации инициируется служебная проверка, проводимая комиссией, состав которой определяется ответственным за организацию обработки персональных данных. По факту выясненных обстоятельств составляется акт расследования инцидента и передается руководителю структурного подразделения для принятия мер согласно локальным нормативным актам Образования и действующему законодательству РФ.

**8.11.** При отправке или передаче персональных данных адресатам на съемные носители записываются только предназначенные адресатам данные.

**8.12.** Вынос съемных носителей персональных данных для непосредственной передачи адресату осуществляется только с

письменного разрешения руководителя структурного подразделения.

**8.13.** Съёмные носители персональных данных, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съёмных носителей с персональными данными осуществляется комиссией, состав которой определяется ответственным за организацию обработки персональных данных. По результатам уничтожения носителей составляется акт.

**8.14.** В случае увольнения или перевода работника в другое структурное подразделение, предоставленные носители персональных данных изымаются и делаются соответствующие пометки в журнале учета машинных носителей.

## **9. Права пользователя**

**9.1.** Использовать ИСПДн Образования для выполнения должностных обязанностей.

**9.2.** Обращаться к ответственному за организацию обработки персональных данных для консультаций по поводу использования программного обеспечения и АРМ, вопросам обработки персональных данных.

**9.3.** Направлять предложения по установке новых версий существующего программного обеспечения (с обоснованием необходимости замены старых версий на новые).

**9.4.** Направлять предложения по модернизации программного обеспечения, разрабатываемого в Образовании или по заказу Образования.

**9.5.** Направлять предложения по установке нового (а также дополнительного) программного обеспечения (с указанием цели использования, преимуществ перед существующими аналогами).

**9.6.** Направлять предложения по модернизации АРМ (замены на новые аналоги), с обязательным обоснованием замены и указанием преимуществ перед существующими аналогами.

**9.7.** Получать консультации и разъяснения по нормативным документам, регламентирующим работу с персональными данными в Образовании.

## **10. Ответственность**

**10.1.** Пользователь несет персональную ответственность за свои действия или бездействие, которые могут повлечь за собой разглашение персональных данных, а также за нарушение нормального функционирования ИСПДн или их отдельных компонентов, несанкционированный доступ к информации в соответствии с законодательством Российской Федерации и локальными нормативными актами Образования.

Лист ознакомления с инструкцией пользователя по работе с  
персональными данными в ГИС ЭО

№ п/ п	ФИО	Должность	Подпись, дата
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			