

Муниципальное бюджетное общеобразовательное учреждение
Петрозаводского городского округа
«Средняя общеобразовательная школа № 25»
Республика Карелия, г. Петрозаводск, наб. Гюллинга, д.3,
1001034808, 1031000007180



Регламент
допуска работников
МОУ «Средняя школа № 25»
к обработке персональных данных

1. Общие положения

1.1. Регламент допуска работников МОУ «Средняя школа № 25» (далее - Регламент, Организация, Работодатель) к обработке персональных данных работников Организации разработан в соответствии с Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных", иными нормативными правовыми актами Российской Федерации и Уставом Организации.

1.2. Настоящий Регламент определяет порядок допуска работников Организации к обработке персональных данных и гарантии обеспечения конфиденциальности сведений о субъекте, предоставленных для обработки.

1.3. Регламент обязателен для исполнения всеми работниками, допущенными к обработке персональных данных. Нарушение Регламента является дисциплинарным нарушением.

1.4. В структурных подразделениях Организации, работники которых осуществляют обработку персональных данных, разрабатываются и представляются на утверждение ответственному за организацию обработки персональных данных в Организации инструкции о порядке обработки персональных данных в соответствующем структурном подразделении Организации.

1.5. Все работники, на которых распространяются положения данного Регламента и инструкций о порядке обработки персональных данных, обязаны ознакомиться с ними под подпись.

1.6. Настоящий Регламент вступает в действие с момента его утверждения приказом руководителя Организации и действует до утверждения нового Регламента.

1.7. Все изменения и дополнения к настоящему Регламенту должны быть утверждены приказом руководителя Организации.

2. Работники, допускаемые к обработке персональных данных

2.1. К обработке персональных данных беспрепятственно допускаются:

руководитель Организации;

заместители руководителя Организации;

специалист по кадрам Организации;

секретарь учебной части Организации;

инженер Организации;

2.2. Наряду с лицами, указанными в п. 2.1 Регламента, к обработке персональных данных, как с использованием средств автоматизации, так и без использования средств автоматизации, включая: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление и/или изменение), извлечение, использование, передачу (распространение, предоставление и/или доступ), обезличивание, блокирование, удаление, уничтожение персональных данных, допускаются только работники, в должностные обязанности которых входит обработка персональных данных (специально уполномоченные лица).

2.2.1. Доступ к персональным данным специально уполномоченным лицам разрешает руководитель Организации по представлению лиц, указанных в п. 2.1 Регламента. В представлении должны быть указаны:

цель допуска к обработке персональных данных;

перечень персональных данных, доступ к обработке которых необходим;

обоснование необходимости и целесообразности допуска к обработке персональных данных;

срок допуска.

2.2.2. Специально уполномоченные лица должны иметь право доступа только к тем персональным данным работника, которые необходимы для выполнения конкретных должностных функций.

2.2.3. Списки специально уполномоченных лиц оформляются в виде отдельного документа.

2.2.4. Оригиналы представлений о допуске специально уполномоченных лиц к обработке персональных данных подлежат хранению для использования в следующих случаях:

восстановление полномочий пользователей - лиц, допущенных к обработке персональных данных после сбоя в информационной системе обработки персональных данных (далее - ИСПДн);

контроль правомерности наличия у конкретного пользователя прав доступа к тем или иным ресурсам ИСПДн при разборе конфликтных ситуаций;

проверка правильности настройки средств разграничения доступа к ресурсам ИСПДн.

2.2.5. При необходимости уполномоченный работник (администратор) в соответствии с назначаемыми правами доступа осуществляет настройку телекоммуникационных средств ИСПДн в части контроля доступа пользователей.

2.2.6. Работнику, зарегистрированному в качестве нового пользователя системы, под роспись (подпись) доводится имя соответствующего ему пользователя и начальное значение пароля, которое он обязан сменить при первом же входе в систему (при первом подключении к ИСПДн).

2.3. Основанием для изменения либо прекращения (отзыва) прав доступа специально

уполномоченного лица является заполненная в установленном порядке письменная Заявка, подписанная лицом, указанным в п. 2.1 Регламента, а также истечение указанного в пп. 2.2.1 п. 2.2 срока допуска.

2.3.1. При изменении должностных обязанностей работника, связанных с переводом в другое подразделение, переводом на другую должность и т.п., учетная запись пользователя на основании заявки лица, указанного в п. 2.1 Регламента, подлежит изменению (корректировке), при этом прежние полномочия аннулируются.

2.3.2. Администратор ИСПДн проводит регистрацию прав доступа к ресурсам указанных в заявке рабочих станций (автоматизированных рабочих мест) с отметкой изменений доступа и другие необходимые операции.

2.3.3. После внесения изменений доступа администратор безопасности информации производит настройку (при их наличии) специализированных средств защиты рабочих станций (автоматизированных рабочих мест).

3. Порядок допуска работников Организации к обработке персональных данных

3.1. Должностные лица, указанные в п. п. 2.1 и 2.2 настоящего Регламента, допускаются к обработке персональных данных субъектов персональных данных с соблюдением общей процедуры оформления работы с персональными данными, предусмотренной действующим законодательством и локальными актами Организации.

3.2. Основаниями для допуска работника к обработке персональных данных являются:

1) приказ о назначении на должность, включенную в перечень должностей руководящих работников Организации, уполномоченных на обработку персональных данных в Организации, либо приказ о назначении на должность, при замещении которой должностной инструкцией (приказом о распределении обязанностей или иным организационно-распорядительным документом подразделения Организации) определены в том числе функции, обязанности и ответственность, связанные с обработкой персональных данных;

2) обязательство о неразглашении персональных данных, составленное по форме согласно Приложению №9, подписанное работником и хранящееся в его личном деле или в деле в соответствии с утвержденной номенклатурой дел подразделения Организации.

3.3. Для организации обработки и обеспечения безопасности персональных данных в Организации руководитель Организации назначает из числа своих заместителей ответственного за организацию обработки персональных данных в Организации.

3.4. Руководители подразделений Организации для организации обработки персональных данных в подразделениях Организации:

1) назначают приказом из числа своих заместителей ответственного за организацию обработки персональных данных в подразделении Организации;

2) обеспечивают до предоставления доступа к обработке персональных данных ознакомление ответственного за организацию обработки персональных данных в подразделении Организации и уполномоченных работников под подпись с законодательством Российской Федерации, нормативными документами Организации в области персональных данных и настоящим Регламентом;

3) утверждают списки уполномоченных работников;

4) утверждают перечни помещений, в которых обрабатываются персональные данные (хранятся материальные носители персональных данных).

3.5. Доступ к информационным системам Организации, в которых обрабатываются персональные данные, предоставляется уполномоченным работникам для выполнения функций, предусмотренных их должностными инструкциями (приказом о распределении обязанностей), и осуществляется в установленном Организации порядке.

3.5.1. Доступ к персональным данным не может быть ограничен пользователями по техническим причинам, в том числе по скорости обработки информации.

3.6. К помещениям, в которых ведется обработка персональных данных, относятся помещения, в которых происходит обработка персональных данных, как с использованием средств автоматизации, так и без использования средств автоматизации, а также хранятся носители персональных данных.

3.6.1. Для помещений, в которых ведется обработка персональных данных, организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей информации, содержащих персональные данные, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц. Данный режим должен обеспечиваться в том числе:

запираем помещения на ключ, в том числе при выходе из него в рабочее время;

закрываем шкафов (ящиков, хранилищ), где хранятся носители информации, содержащие персональные данные, во время отсутствия в помещении уполномоченных на обработку персональных данных.

3.6.2. Нахождение лиц, не имеющих права на осуществление обработки персональных данных либо на осуществление доступа к персональным данным, в помещениях, в которых ведется обработка персональных данных, возможно только в сопровождении уполномоченного на обработку персональных данных на время, ограниченное необходимостью решения служебных вопросов.

4. Блокирование, отзыв прав доступа

4.1. Блокирование учетных записей на время отпуска пользователей ИСПДн осуществляется администратором по заявке начальника соответствующего структурного подразделения. Учетная запись пользователя может быть временно разблокирована, либо изменены права доступа по заявке начальника структурного подразделения, в котором работает пользователь.

4.2. Допуск к обработке персональных данных работников Организации прекращается:

при истечении указанного в пп. 2.2.1 п. 2.2 срока допуска;

при увольнении работника Организации, имеющего допуск;

при переводе работника Организации, имеющего допуск, на должность, выполнение работ по которой уже не требует допуска к обработке персональных данных.

4.3. Допуск к обработке персональных данных у лиц, указанных в п. 2.2 настоящего Регламента, может быть дополнительно прекращен по письменному решению руководителя

Организации или уполномоченного им лица.

4.4. При увольнении работников и/или лишении их прав доступа к персональным данным начальник структурного подразделения, в котором работает такой работник, подает Заявку на имя руководителя Организации. Руководитель Организации визирует Заявку, утверждая тем самым лишение прав пользователя на доступ к персональным данным.

4.5. После визирования Заявка на бумажном носителе или в электронном виде поступает к соответствующему администратору ИСПДн и администратору безопасности информации.

4.6. Администратор ИСПДн удаляет учетные записи из всех указанных в Заявке списков доступа.

4.7. Администратор безопасности информации:

проводит смену (удаление) действующих настроек прав доступа на соответствующих средствах защиты в соответствии с изменившимися полномочиями;

производит необходимые отметки в учетных реестрах;

совместно с непосредственным руководителем работника анализирует целостность данных, к которым имел доступ работник.

4.8. Администратор безопасности информации вместе с администратором ИСПДн анализирует автоматизированное рабочее место уволенного работника на наличие закладок, вирусов, после чего все данные на жестком диске работника уничтожаются и операционная система (ОС) на рабочем месте переинсталлируется.

4.9. Все изменения в правах доступа, связанные с увольнением пользователя, выполняются администраторами не позднее трех суток с момента получения заявки на внесение изменений.

5. Порядок и периодичность проверки прав пользователей

5.1. Проверка прав пользователей проводится администратором безопасности информации с периодичностью не реже одного раза в три месяца(ев) путем сравнения прав согласно утвержденному списку.

6. Ответственность

6.1. Ответственные за обработку персональных данных обязаны соблюдать следующие требования (за исключением случаев обезличивания персональных данных и в отношении общедоступных персональных данных):

а) объем и содержание обрабатываемых персональных данных, способы их обработки должны соответствовать целям обработки персональных данных;

б) защита персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных обеспечивается в порядке, установленном нормативными правовыми актами Российской Федерации;

в) обеспечение конфиденциальности персональных данных.