



МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
НАЧАЛЬНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 7
ГОРОДА ЮЖНО-САХАЛИНСКА

693007, г. Южно-Сахалинск, ул. им. Антона Буюклы, 14,
Тел.: (4242) 22-54-75, (4242) 22-54-76, факс: (4242) 22-54-76 Email: school7@yuzhno-sakh.ru

УТВЕРЖДЕНЫ

приказом директором
Муниципального автономного
образовательного учреждения
начальная общеобразовательная
школа №7 города Южно-Сахалинска
от 16.05.2016 № 120 – ОД

ПРАВИЛА
обработки персональных данных

1. Общие положения

1.1. Данные Правила предназначена для использования сотрудниками допущенными к работе с персональными данными Муниципального автономного общеобразовательного учреждения начальная общеобразовательная школа №7 города Южно-Сахалинска (далее - ОУ).

1.2. Отнесение информации к сведениям, содержащим персональные данные, осуществляется в соответствии с «Перечнем сведений, содержащих персональные данные и правовыми основаниями обработки персональных данных».

1.3. Сотрудники ОУ, доступ которых к персональным данным необходим для выполнения ими своих служебных (трудовых) обязанностей, должны быть ознакомлены под подпись с настоящими Правилами и предупреждены о возможной ответственности за её нарушение.

2. Термины и определения

2.1. **Информация** - сведения (сообщения, данные) независимо от формы их представления (ст. 2 ФЗ РФ от 27.07.2006 г. N 149-ФЗ «Об информации, информационных технологиях и защите информации»).

2.2. **Доступ к информации** – возможность получения информации и её использования (ст. 2 ФЗ РФ от 27.07.2006 г. N 149-ФЗ «Об информации, информационных технологиях и защите информации»).

2.3. **Носитель информации** - любой материальный объект или среда, используемый для хранения или передачи информации.

2.4. **Несанкционированный доступ (НСД)** – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путём изменения (повышения, фальсификации) своих прав доступа.

2.5. Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств (*ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»*).

2.6. 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 (*ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»*).

2.7. Пароль – секретная комбинация цифр, знаков, слов, или осмысленное предложение, служащие для защиты информации от несанкционированного доступа к информационным ресурсам.

2.8. Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (*ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»*).

2.9. Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц (*ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»*).

2.10. Субъект персональных данных — физическое лицо, которое прямо или косвенно определено или определяется с помощью персональных данных

2.11. 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 (*ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»*).

3. Порядок работы со сведениями, содержащими персональные данные

3.1. При обработке персональных данных на бумажных носителях, съёмных носителях (дискетах, дисках, флеш-носителях и т.п.), компьютерах и других технических средствах, сотрудники ОУ обязаны следить как за сохранностью самих бумажных документов, съёмных носителей и компьютеров и других технических средств, так и за сохранностью содержащейся в них информации, а именно не допускать неправомерного ознакомления с ней лиц, не имеющих допуска к работе с персональными данными.

3.2. Запрещается хранение или оставление бумажных документов и съёмных носителей, содержащих персональные данные, в виде, позволяющем осуществить визуальный просмотр содержащихся в них персональных данных, их фотографирование или несанкционированное создание копий. Напечатанные документы, содержащие персональные данные, должны изыматься из принтеров немедленно. Хранение бумажных документов и съёмных носителей, содержащих персональные данные, допускается только в специальных закрытых шкафах, сейфах и помещениях, к которым исключён доступ лиц, не допущенных к обработке соответствующих персональных данных.

3.3. Запрещается без прямой служебной необходимости делать выписки персональных данных, распечатывать документы с персональными данными или записывать персональные данные на съёмные носители.

3.4. Запрещается использовать для передачи персональных данных съёмные носители, не учтённые в «Журнале учета съёмных носителей информации».

3.5. Запрещается выносить документы, съёмные носители или переносные компьютеры, содержащие персональные данные, за пределы служебных помещений ОУ, если это не требуется для выполнения служебных (трудовых) обязанностей и если на это

не дано разрешение директора ОУ или ответственного за организацию обработки персональных данных.

3.6. Бумажные документы с персональными данными, у которых истёк срок хранения, лишние или испорченные копии документов с персональными данными, должны быть уничтожены без возможности их восстановления (например, в shredders).

3.7. Большие объёмы бумажных документов с персональными данными, съёмные носители с персональными данными, а также встроенные в компьютеры носители с персональными данными должны уничтожаться под контролем ответственного за организацию обработки персональных данных, способом, исключающим дальнейшее восстановление информации.

3.8. Мониторы компьютеров, используемых для обработки персональных данных, должны быть ориентированы таким образом, чтобы исключить визуальный просмотр информации с них лицами, не имеющими допуск к обработке персональных данных.

3.9. Запрещается упоминать в разговоре с третьими лицами сведения, содержащие персональные данные.

3.10. Запрещается в нерабочее время или за пределами служебных помещений упоминать в разговоре с кем-либо, включая любых сотрудников ОУ, сведения, содержащие персональные данные.

3.11. Запрещается обсуждать порядок доступа, места хранения, средства и методы защиты персональных данных с кем-либо, кроме ответственного за организацию обработки персональных данных, администратора безопасности ИСПДн, руководства, или лица, уполномоченного руководством на обсуждение данных вопросов.

4. Порядок доступа лиц в помещения

4.1. При обеспечении доступа лиц соблюдаются требования законодательства РФ по защите персональных данных.

4.2. Обеспечение доступа лиц в помещения предусматривает комплекс специальных мер, направленных на поддержание и обеспечение установленного порядка деятельности структурных подразделений и определяет порядок пропуска сотрудников ОУ и иных третьих лиц в помещения.

4.3. В случаях, не терпящих отлагательства (пожар, авария систем тепло-, водоснабжения и т.п.), когда находящимся в помещении оборудованию, материальным ценностям и документации грозит опасность уничтожения или вывода из строя, сотрудник оповещает пожарную охрану (аварийную службу), вызывает руководителя, работника, ответственного за помещение. Служебное помещение вскрывается до прибытия указанных лиц, и принимаются меры к тушению пожара (ликвидации аварии), эвакуации ценностей, имущества и документации. Около эвакуируемых ценностей, имущества и документации выставляется временный пост охраны. Акт о вскрытии помещения составляется после окончания работ, связанных с ликвидацией происшествия.

4.4. Нахождение посетителей допускается только в рабочее время.

4.5. В помещения ИСПДн пропускаются:

4.5.1. беспрепятственно – директор и сотрудники, имеющие допуск к работе с персональными данными и с целью выполнения должностных обязанностей;

4.5.2. с разрешения директора ОУ, в сопровождении ответственного за организацию обработки персональных данных, сотрудники контролирующих органов, сотрудники пожарных и аварийных служб, сотрудники полиции;

4.5.3. ограниченно - сотрудники, не имеющие допуска к работе с персональными данными или не имеющие функциональных обязанностей в помещении, сотрудники сторонних организаций и учреждений для выполнения договорных отношений.

4.6. Посетители пропускаются в помещения ИСПДн ОУ в рабочее время в сопровождении сотрудников, допущенных к обработке персональных данных.

4.7. В помещениях, в которых происходит обработка персональных данных, запрещено использование не предусмотренных служебными обязанностями технических устройств, фотографирование, видеозапись, звукозапись, в том числе с использованием мобильных телефонов.

4.8. Рабочие и специалисты ремонтно-строительных организаций пропускаются в помещение для проведения ремонтно-строительных работ на основании заявок, подписанных директором ОУ.

4.9. В целях предотвращения несанкционированного доступа к сведениям, содержащим персональные данные, работы проводятся только под контролем ответственного за организацию обработки персональных данных.

4.10. Контроль за допуском в служебные помещения в рабочее время возлагается на сотрудников работающих в данном помещении. В нерабочее время, выходные и нерабочие праздничные дни охрана служебных помещений обеспечивается контрольно-пропускным режимом в соответствии с порядком и правилами внутриобъектового пропускного режима, средствами охранной сигнализации.

4.11. Для исключения возможности бесконтрольного проникновения в помещения и к установленному в них оборудованию посторонних лиц, двери в отсутствие штатных сотрудников запираются на ключ.

4.12. Помещения, где хранятся персональные данные, защищаемые криптографическими средствами защиты информации, должны быть оснащены входными дверьми с замками для обеспечения постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода. Помещения должны опечатываться по окончании рабочего дня или быть оборудованы соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии помещений

4.13. Сотрудники, уполномоченные хранить ключи от сейфов и помещений должны вести «Журнал учета ключей от сейфов и помещений».

4.14. Оборудование в помещении должно размещаться таким образом, чтобы исключить возможность бесконтрольного доступа к нему посторонних лиц.

4.15. Окна помещений, в которых ведётся обработка персональных данных, должны быть оборудованы шторами или жалюзи.

4.16. Уборка помещений ИСПДн должна производиться под контролем сотрудника, допущенного к обработке персональных данных в этом помещении.

4.17. Во время уборки в помещении должна быть приостановлена работа с персональными данными, должны быть выключены или заблокированы все АРМ, на которых обрабатываются персональные данные. Носители, содержащие персональные данные, должны быть убраны в закрытые шкафы или сейфы.

5. Действия при обнаружении попыток несанкционированного доступа

5.1. К попыткам несанкционированного доступа относятся:

5.1.1. сеансы работы с персональными данными незарегистрированных пользователей, или пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истёк, или превышающих свои полномочия по доступу к данным;

5.1.2. действия третьего лица, пытающегося получить доступ (или уже получившего доступ) к ИСПДн, при использовании учётной записи администратора или другого пользователя ИСПДн, методом подбора пароля, использования личного пароля, разглашённого владельцем учётной записи или любым другим методом.

5.2. При выявлении факта несанкционированного доступа пользователь ИСПДн обязан:

5.2.1. прекратить несанкционированный доступ к персональным данным;

5.2.2. доложить директору ОУ запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;

5.2.3. известить администратора безопасности ИСПДн и ответственного за организацию обработки ПДн о факте несанкционированного доступа.

6. Требования по техническому укреплению

6.1.1. Двери и окна должны иметь прочные и надежные петли, шпингалеты, крючки или задвижки и быть плотно подогнаны к рамам и дверным коробам. Допускается применение электромеханических, электромагнитных замков и задвижек.

6.1.2. Конструкция оконных рам должна исключать возможность демонтажа с наружной стороны оконного проема стекол.

6.1.3. Стекла в рамах должны быть надежно закреплены в пазах.

6.1.4. Рамы указанных оконных проемов оборудуются запорными устройствами.

7. Ответственность за разглашение персональных данных

7.1. Сотрудники ОУ, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъектов, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

7.2. Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе другим сотрудникам, не имеющим к ним доступ), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных локальными нормативно-правовыми актами (приказами, распоряжениями) ОУ, влечет наложение на сотрудника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Сотрудник ОУ, имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба ОУ (в соответствии с п.7 ст. 243 Трудового кодекса РФ).

7.2.1. В отдельных случаях, при разглашении персональных данных, сотрудник, совершивший указанный проступок, несет ответственность в соответствии со статьей 13.14 Кодекса об административных правонарушениях РФ.

7.3. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии со ст. 137 Уголовного кодекса РФ.

7.4. Директор ОУ за нарушение норм, регулирующих получение, обработку и защиту персональных данных субъектов, несет административную ответственность согласно ст. 5.27 и 5.39 Кодекса об административных правонарушениях Российской Федерации, а также возмещает субъекту ущерб, причиненный неправомерным использованием информации, содержащей персональные данные этого субъекта.