МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«ЦОЦИ-ЮРТОВСКАЯ СРЕДНЯЯ ШКОЛА №1 ИМ. ХАМЕРЗАЕВА Х.А.»

Согласовано
Совет школы
от 28. 08.2017г. № 1

Утверждаю
Директор МБОУ «Цоци-Юртовская
СШ №1 им. Хамерзаева Х.А.»
_____ З.А.Гисаева

Согласовано
Протокол заседания Совета родителей
от 26. 08.2017г. № 1

Утверждено
приказом МБОУ «Цоци-Юртовская
СШ № 1 им. Хамерзаева Х.А.»
от 05 сентября № 131

Согласовано
Протокол заседания Совета обучающихся
от 28. 08.2017г. № 1

Положение
о порядке обработки и обеспечении безопасности персональных данных

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с Федеральным законом «О персональных данных» (далее – Федеральный закон), 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 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

1.2. В целях настоящего Положения используются следующие термины и понятия:

персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;

информационная система персональных данных - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;
обработка персональных данных без использования средств автоматизации (неавтоматизированная) - обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Основные условия проведения обработки персональных данных

2.1. В организации приказом руководителя назначается лицо, ответственный за защиту персональных данных, и определяется перечень лиц, допущенных к обработке персональных данных.

2.2. Лица, допущенные к обработке персональных данных, в обязательном порядке под роспись знакомятся с настоящим Положением и подписывают обязательство о неразглашение информации, содержащей персональные данные, по форме согласно приложению №2 к настоящему Положению.

2.3. Запрещается:
обрабатывать персональные данные в присутствии лиц, не допущенных к их обработке;
осуществлять ввод персональных данных под диктовку.

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

3.1. Обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации осуществляется в соответствии с требованиями постановления Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

3.2. Оператором осуществляется классификация информационных систем персональных данных в соответствии с Приказом ФСТЭК России, ФСБ России, Мининформ связи России от 13.02.2008 № 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных" в зависимости от категории обрабатываемых данных и их количества.

3.3. Мероприятия по обеспечению безопасности персональных данных на стадиях проектирования и ввода в эксплуатацию объектов информатизации проводятся в соответствии с приказом ФСТЭК Росси от 05.02.2010 №58 «О методах и способах защиты информации в информационных системах персональных данных».

3.4. Не допускается обработка персональных данных в информационных системах персональных данных 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, 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.

4. Порядок обработки персональных данных без использования средств автоматизации

4.1. 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.

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

4.3. При неавтоматизированной обработке персональных данных на бумажных носителях:
не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо не совместимы;
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.

4.4. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных
(далее - типовые формы), должны соблюдаться следующие условия:
а) 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;
б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных, - при необходимости получения письменного согласия на обработку персональных данных;
в) 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;
г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.
4.5. Неавтоматизированная обработка персональных данных в электронном виде осуществляется на внешних электронных носителях информации.
4.6. При отсутствии технологической возможности осуществления неавтоматизированной обработки персональных данных в электронном виде на внешних носителях информации необходимо принимать организационные (охрана помещений) и технические меры (установка сертифицированных средств защиты информации), исключающие возможность несанкционированного доступа к персональным данным лиц, не допущенных к их обработке.
4.7. Электронные носители информации, содержащие персональные данные, учитываются в журнале учета электронных носителей персональных данных, составленном по форме согласно приложению №3 к настоящему Положению.
К каждому электронному носителю оформляется опись файлов, содержащихся на нем, с указанием цели обработки и категории персональных данных.
4.8. При несовместимости целей неавтоматизированной обработки персональных данных, зафиксированных на одном электронном носителе, если электронный 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:
а) 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;
б) 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.
4.9. Документы и внешние электронные носители информации, содержащие персональные данные, должны храниться в служебных помещениях в охраняемых шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.
4.10. 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).

5. Обязанности и права субъектов персональных данных
5.1. В целях обеспечения достоверности персональных данных, Клиент обязан:
5.1.1. При заключении договора предоставить Обществу полные и достоверные данные о себе.
5.1.2. В случае изменения сведений, составляющих персональные данные клиента, незамедлительно, но не позднее пяти рабочих дней, предоставить данную информацию Обществу.
5.2. Общество обязано:
5.2.1. Обеспечить защиту персональных данных своих клиентов от неправомерного их использования или утраты в порядке, установленном законодательством РФ.
5.2.2. Определить политику в отношении обработки персональных данных клиентов и контрагентов.
5.2.3. Предоставить возможность клиенту или его представителям беспрепятственно ознакамливаться с настоящим Положением и его правами в области защиты персональных данных.
5.2.4. Обеспечить хранение первичной учетной документации. При этом персональные данные не должны храниться дольше, чем это оправдано выполнением задач, для которых они собирались, или дольше, чем это требуется в интересах лиц, о которых собраны данные.
5.2.5. В случае реорганизации или ликвидации Оператора учет и сохранность документов, порядок передачи их на дальнейшее хранение осуществлять в соответствии с правилами, предусмотренными учредительными документами и действующим законодательством Российской Федерации.
5.2.6. Осуществлять передачу персональных данных субъекта только в соответствии с настоящим Положением и законодательством Российской Федерации.
5.2.7. По требованию субъекта или его законного представителя предоставить ему полную информацию о его персональных данных и обработке этих данных.

5.2.8. По требованию уполномоченного органа по защите прав субъектов персональных данных предоставлять документы и локальные акты Общества.
5.3. В целях обеспечения защиты персональных данных, хранящихся у Общества, Клиенты имеют право на:
5.3.1. Полную информацию о составе персональных данных и их обработке, в частности клиент имеет право знать, кто и в каких целях использует или использовал информацию о его персональных данных.
5.3.2. Свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные клиента или контрагента, за исключением случаев, предусмотренных законодательством РФ.
5.3.3. Определение своих представителей для защиты своих персональных данных.
5.3.4. Требование об уточнении, исключении или исправлении неверных или неполных устаревших, недостоверных, незаконно полученных или не являющихся необходимыми для Общества персональных данных. При отказе Общества исключить или исправить персональные данные клиент имеет право заявить в письменной форме Обществу о своем несогласии с соответствующим обоснованием такого несогласия.
5.3.5. Требование об извещении Обществом всех лиц, которым ранее были сообщены неверные или неполные персональные данные клиента, обо всех произведенных в них исключениях, исправлениях или дополнениях.
5.3.6. Обжалование в суд любых неправомерных действий или бездействия Общества при обработке и защите его персональных данных.

6. Обеспечение безопасности персональных данных

6.1. Безопасность персональных данных, обрабатываемых Обществом, обеспечивается реализацией правовых, организационных, технических и программных мер, необходимых и достаточных для обеспечения требований федерального законодательства в области защиты персональных данных.
6.2. Общество предпринимает необходимые организационные и технические меры для обеспечения безопасности персональных данных от случайного или несанкционированного доступа, уничтожения, изменения, блокирования доступа и других несанкционированных действий.
6.3. Общество применяет следующие организационные и технические меры:
- назначение должностных лиц, ответственных за организацию обработки и защиты персональных данных;
- ограничение и регламентация состава работников, имеющих доступ к персональным данным;
- ознакомление работников с требованиями федерального законодательства и нормативных документов Общества по обработке и защите персональных данных;
- обеспечение учета и хранения материальных носителей информации и их обращения, исключающего хищение, подмену, несанкционированное копирование и уничтожение;

- определение угроз безопасности персональных данных при их обработке, формирование на их основе моделей угроз;
- разработка на основе модели угроз системы защиты персональных данных для соответствующего класса информационных систем;
- реализация разрешительной системы доступа пользователей к информационным ресурсам, программно-аппаратным средствам обработки и защиты информации;
- парольная защита доступа пользователей к информационной системе персональных данных;
- применение средств контроля доступа к коммуникационным портам, устройствам ввода-вывода информации, съемным машинным носителям и внешним накопителям информации;
- осуществление антивирусного контроля, предотвращение внедрения в корпоративную сеть вредоносных программ (программ-вирусов) и программных закладок;
- применение межсетевого экранирования;
- обнаружение вторжений в корпоративную сеть Оператора, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных;
- резервное копирование информации;
- обеспечение восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- обучение работников, использующих средства защиты информации, применяемые в информационных системах персональных данных, правилам работы с ними;
-учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;
- размещение технических средств обработки персональных данных, в пределах охраняемой территории;
поддержание технических средств охраны, сигнализации помещений в состоянии постоянной готовности.

7. Ответственность должностных лиц

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