СОГЛАСОВАНО
Председатель профкома БОУ ДО
г. Омска «Детский ЭкоЦентр»

_____ Е.Н. Кистенева
«_9_» _____ 20_16_ г.

УТВЕРЖДАЮ
Директор БОУ ДО
г. Омска «Детский ЭкоЦентр»

_____ Г.В. Ситникова
«_9_» _____ 20_16_ г.

Принято на общем собрании трудового коллектива
Протокол № _2_
«_9_» _____ 20_16_ г.

РЕГЛАМЕНТ ПРОЦЕДУР, ПРЕПЯТСТВУЮЩИХ НЕСАНКЦИОНИРОВАННОМУ ДОСТУПУ К ПЕРСОНАЛЬНЫМ ДАННЫМ РАБОТНИКОВ БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ ГОРОДА ОМСКА «ДЕТСКИЙ ЭКОЛОГО-БИОЛОГИЧЕСКИЙ ЦЕНТР»

1. Общие положения

1.1. Настоящий Перечень мер, направленных на предотвращение неправомерного использования персональных данных работников (далее – Перечень мер) бюджетного образовательного учреждения дополнительного образования города Омска «Детский Эколого-биологический Центр» (далее – Учреждение) определяет порядок противодействия несанкционированному использованию персональных данных сотрудниками, имеющими доступ к такой информации, а также их ответственность, в случае совершения ими действий, повлекших неправомерное использование персональных данных.

1.2. Целью настоящего документа является установление в Учреждении процедур, позволяющих:

- исключить возможность несанкционированного доступа к персональным данным и их использования работниками Учреждения и третьими лицами в собственных интересах в ущерб интересам граждан.

Перечень, а также изменения и дополнения к нему рассматриваются и утверждаются директором Учреждения.

2. Термины и определения

В настоящем перечне мер применяются следующие термины и определения:

2.1. Персональные данные (ПД) – любая информация, относящаяся к определённому или определяемому на основании такой информации физическому лицу (субъекту ПД), в том числе: фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

2.2. Оператор персональных данных – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание такой обработки.

2.3. 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 наличия таких средств.

2.4. 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.

Применяемые в Перечне мер понятия и определения, не приведенные в настоящем разделе, используются в соответствии с понятиями и определениями, содержащимися в законодательстве Российской Федерации.

3. Общие положения о персональных данных и порядке их использования

3.1. Персональные данные могут быть представлены в различном виде, в том числе в бумажном или электронном.

3.2. Персональные данные могут передаваться только тем лицам, которым они необходимы для исполнения ими своих прямых должностных обязанностей.

3.3. Сотрудники Учреждения, осуществляющие проведение, обработку и учёт персональных данных не имеют права передавать данную информацию третьим лицам и работникам Учреждения, режим доступа которых не предусматривает возможности обладания такой информацией, либо использовать её в личных целях.

3.4. За использование и разглашение персональных данных, сотрудник Учреждения несёт персональную ответственность в соответствии с должностной инструкцией и действующим законодательством РФ.

4. Основные меры (процедуры) препятствующие несанкционированному использованию персональных данных

4.1. Под процедурами, препятствующими несанкционированному использованию персональных данных, в целях реализации настоящего документа, понимаются мероприятия по предупреждению несанкционированного использования, оперативному и последующему контролю использования персональных данных, проводимые сотрудниками Учреждения.

4.2. Учреждением применяются следующие меры, препятствующие несанкционированному доступу к персональным данным:

- ограничение доступа к персональным данным в специализированных программных средствах;
- защита персональных данных при их обработке и архивировании;
- ограничение доступа посторонних лиц в помещение Учреждения, предназначенные для осуществления работы с ПД;
- защита рабочих мест работников, осуществляющих операции с программными средствами;
- контроль за соблюдением работниками Учреждения требований законодательства РФ и иных нормативных правовых актов.

4.3. В целях противодействия несанкционированному использованию персональных данных, предотвращения утечки и обеспечения сохранности персональных данных учреждение использует следующий комплекс мероприятий:

- ограничение доступа к служебной информации в программных средствах;
- обеспечение доступа к данным только в пределах полномочий, представленных непосредственно исполнителям, обеспечивающим ведение, обработку и учёт информации с ПД;
- установление индивидуальных кодов и паролей доступа к данным для каждого исполнителя;
- осуществление административных и технических мер, направленных на исключение несанкционированного доступа к данным; блокирование доступа пользователя в систему, в случае обнаружения попыток несанкционированного доступа, установка программных средств, оповещающих ответственного за организацию работы по обеспечению защиты информации о попытке несанкционированного доступа, блокировка рабочего места нарушителя;

- контроль за соблюдением режима обращения ПД осуществляется ответственным за организацию работы по обеспечению защиты информации, а также директором Учреждения;

4.3.1. Защита ПД при её обработке и архивировании:

- обеспечение дублирования данных в процессе их ввода, предусматривающее сохранность первичного носителя информации;
- установка программных средств для создания резервных копий, способствующих быстрому восстановлению данных;
- использование систем защиты информационно-технических систем и каналов связи от утечки персональных данных;
- осуществление резервного копирования (восстановления) только уполномоченными сотрудниками.

4.3.2. Ограничение доступа посторонних лиц в помещении Учреждения, предназначенные для осуществления сбора, обработки и хранения информации ПД осуществляется за счёт:

- соблюдения порядка и правил доступа в служебные помещения в соответствии с Положением о защите ПД работников Учреждения, утверждённым директором;
- ограничение доступа работников и посторонних лиц в помещении, в котором размещены персональные компьютеры, вычислительные системы и системы телекоммуникаций для осуществления операций с ПД.

4.3.3. Защита рабочих мест работников, осуществляющих сбор и обработку ПД:

- защита окон в служебных помещениях от внешнего дистанционного наблюдения жалюзи и шторами;
- эффективное размещение рабочих мест сотрудников для исключения возможности несанкционированного просмотра документов и информации на мониторах;
- соблюдение сотрудниками подразделений правил по обеспечению защиты информации при работе с персональными компьютерами.

4.3.4. Ограничение доступа к ПД:

- доступ работников к необходимым документам, только для выполнения своих служебных обязанностей;
- проведение инвентаризации мест хранения документов, содержащих ПД;
- контроль за соблюдением утверждённых внутренних регламентов.

4.3.5. При оформлении на работу в Учреждение, работник даёт расписку о неразглашении ПД.

4.3.6. Контроль за соблюдением работниками Учреждения требований законодательства РФ и иных нормативных правовых актов, регулирующих работу с ПД, внутренними документами, возложен на директора.

5. Осуществление процедур, препятствующих несанкционированному использованию персональных данных, и контроля за их исполнением

5.1. Проведение процедур, препятствующих несанкционированному использованию ПД, и осуществление контроля включает в себя:

5.1.1. Установление требований о неразглашении ПД.

5.1.2.Контроль за выполнением работниками Учреждения требований действующего законодательства РФ и внутренних документов Учреждения.

5.1.3. Уведомление работников Учреждения, имеющих доступ к информации о ПД, о недопустимости осуществления операций с ПД, как в своих интересах, так и в интересах третьих лиц.

5.1.4. Проведение оперативных проверок на предмет возможной утечки персональных данных в случаях, предполагающих несанкционированное использование персональных данных.

5.1.5. Направление сведений руководству Учреждения об установленных (обнаруженных) случаях несанкционированного использования ПД.

6. Ответственность при реализации процедур, препятствующих несанкционированному использованию персональных данных

6.1. Ответственный за организацию работы по обеспечению защиты информации отвечает за:

- осуществление контроля исполнения нормативных документов по вопросам организации и эффективного функционирования системы внутреннего контроля Учреждения;
- контроль исполнения внутренних нормативных документов по вопросам обеспечения конфиденциальности ПД в Учреждении;
- проведение служебных расследований по фактам возможного неправомерного использования работниками Учреждения ПД, о результатах которых ответственный за обеспечение защиты информации незамедлительного уведомляет директора Учреждения.

6.2. Работники, которым стали известны факты неправомерного использования ПД при осуществлении профессиональной деятельности, должны незамедлительно доложить об этом директору Учреждения.

6.3. Ответственность сотрудников и должностных лиц Учреждения за нарушения режима обращения с ПД и порядок наложения взыскания:

6.3.1. Виды взысканий, применяемых к сотрудникам и должностным лицам Учреждения, нарушившим режим обращения с персональными данными:

- замечание;
- выговор;
- увольнение с работы.

6.3.2. Взыскание к сотруднику применяется директором Учреждения.

7. Заключительные положения

7.1. Ответственный за организацию работы по обеспечению защиты информации осуществляет ознакомление сотрудников Учреждения с настоящим Перечнем мер не позднее одного месяца со дня его вступления в силу. Факт ознакомления подтверждается подписью сотрудника. В дальнейшем, проводится регулярный инструктаж сотрудников с периодичностью не реже одного раза в год, с целью неукоснительного соблюдения сотрудниками мероприятий, направленных на предотвращение неправомерного использования ПД при осуществлении Учреждением профессиональной деятельности.

7.2. Ответственный за организацию работы по обеспечению защиты информации, в случае принятия в штат Учреждения нового сотрудника, осуществляет ознакомление с настоящим Перечнем мер не позднее одной недели со дня его зачисления в штат.

7.3. Работники Учреждения должны предпринимать все необходимые меры, позволяющие предотвратить неправомерное распространение и использование ПД при проведении операций, связанных с осуществлением профессиональных видов деятельности.

7.4. Настоящий Перечень мер утверждается директором Учреждения в установленном законодательством порядке.
