УТВЕРЖДАЮ
Директор МБОУ
«СОШ-ДЕТСКИЙ САД № 17»
_____ Е.М. Демидова
Приказ №_1061_
от «23» 10 2019г.

# ИНСТРУКЦИЯ О ПОРЯДКЕ ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ ПРИ ОБРАЩЕНИИ С ИНФОРМАЦИЕЙ, СОДЕРЖАЩЕЙ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция устанавливает применяемые в муниципальном бюджетном общеобразовательном учреждении «Средняя общеобразовательная школа-детский сад № 17 города Евпатории Республики Крым» (далее - Школа) способы обеспечения безопасности при обработке, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, защиту, распространение (в том числе передачу), обезличивание, блокирование, уничтожение, персональных данных с целью соблюдения конфиденциальности сведений, содержащих персональные данные работников и обучающихся Университета.

1.2. Настоящая Инструкция разработана на основании Конституции Российской Федерации, Трудового кодекса Российской Федерации, Федерального закона от 19.12.2005 г. №160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных», Федерального закона РФ от 27.07.2006 № 152-ФЗ «О персональных данных», постановлений 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" и от 15 сентября 2008 г. № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации" и иных нормативных правовых актов Российской Федерации, а также «Положения о персональных данных работников и обучающихся МБОУ «ЗСШ».

1.3. В соответствии с законодательством РФ под персональными данными понимается 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, необходимая Школе в связи с трудовыми отношениями и организацией образовательного процесса.

1.4. Требование обеспечения конфиденциальности при обработке персональных данных означает обязательное для соблюдения должностными лицами Школы, допущенными к обработке персональных данных, иными получившими доступ к персональным данным лицами требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

1.5. Обеспечение конфиденциальности персональных данных не требуется в случае:
- обезличивания персональных данных;
- для общедоступных персональных данных.

1.6. Перечни персональных данных и ответственных за хранение и обработку персональных данных указаны в "Положения о персональных данных работников и обучающихся" (пп. 4,6). Обработка и хранение конфиденциальных данных лицами, не указанными в "Положения о персональных данных работников и обучающихся" запрещается.

1.7. В целях обеспечения требований соблюдения конфиденциальности и безопасности при обработке персональных данных Школы предоставляет должностным лицам, работающим с персональными данными, необходимые условия для выполнения указанных требований:

- знакомит работника под роспись с требованиями «Положения о персональных данных работников и обучающихся, с настоящей Инструкцией, с должностной инструкцией и иными локальными нормативными актами Школы в сфере обеспечения конфиденциальности и безопасности персональных данных;
- предоставляет хранилища для документов, средства для доступа к информационным ресурсам (ключи, пароли и т.п.);
- обучает правилам эксплуатации средств защиты информации;
- проводит иные необходимые мероприятия.

1.8. Должностным лицам Школы, работающим с персональными данными, запрещается сообщать их устно или письменно кому бы то ни было, если это не вызвано служебной необходимостью. После подготовки и передачи документа файлы черновиков и вариантов документа переносятся подготовившим их сотрудником на маркированные носители, предназначенные для хранения персональных данных.

Без согласования с руководителем структурного подразделения формирование и хранение баз данных (картотек, файловых архивов и др.), содержащих конфиденциальные данные, запрещается.

1.9. Должностные лица Школы, работающие с персональными данными, обязаны использовать информацию о персональных данных исключительно для целей, связанных с выполнением своих трудовых обязанностей.

1.10. При прекращении выполнения трудовой функции, связанной с обработкой персональных данных, все носители информации, содержащие персональные данные (оригиналы и копии документов, машинные и бумажные носители и пр.), которые находились в распоряжении должностного лица в связи с выполнением должностных обязанностей, данный работник должен передать своему непосредственному руководителю.

1.11. Передача персональных данных третьим лицам допускается только в случаях, установленных законодательством РФ, в соответствии с «Положением о персональных данных работников и воспитанников, обучающихся МБОУ «СОШ-ДЕТСКИЙ САД № 17», с настоящей Инструкцией, должностными инструкциями и иными локальными нормативными актами Школы.

Передача персональных данных осуществляется ответственным за обработку персональных данных должностным лицом Школы на основании письменного или устного поручения руководителя структурного подразделения.

1.12. Передача сведений и документов, содержащих персональные данные, оформляется путем составления акта по установленной настоящей Инструкцией форме (Приложение № 1).

1.13. Должностное лицо, предоставившее персональные данные третьим лицам, направляет письменное уведомление субъекту персональных данных о факте передачи его данных третьим лицам.

1.14. Запрещается передача персональных данных по телефону, факсу, электронной почте за исключением случаев, установленных законодательством и действующими в Школе локальными нормативными актами.

Ответы на запросы граждан и организаций даются в том объеме, который позволяет не разглашать в ответах персональные данные, за исключением данных, содержащихся в материалах заявителя или опубликованных в общедоступных источниках.

1.15. Должностные лица Школы, работающие с персональными данными, обязаны немедленно сообщать директору Школы и заместителю директора по УВР (по безопасности) обо

всех ставших им известными фактах получения третьими лицами несанкционированного доступа либо попытки получения доступа к персональным данным, об утрате или недостаче носителей информации, содержащих персональные данные, удостоверений, пропусков, ключей от сейфов (хранилищ), личных печатей, электронных ключей и других фактах, которые могут привести к несанкционированному доступу к персональным данным, а также о причинах и условиях возможной утечки этих сведений.

1.16. Должностные лица, осуществляющие обработку персональных данных, за невыполнение требований конфиденциальности, защиты персональных данных несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством РФ.

1.17. Отсутствие контроля со стороны Школы за надлежащим исполнением работником своих обязанностей в области обеспечения конфиденциальности и безопасности персональных данных не освобождает работника от таких обязанностей и предусмотренной законодательством РФ ответственности.

## 2. ПОРЯДОК ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

2.1. Обработка персональных данных, в том числе содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такая обработка осуществляется при непосредственном участии человека.

2.2. Руководитель структурного подразделения, осуществляющего обработку персональных данных без использования средств автоматизации:

- определяет места хранения персональных данных (материальных носителей);
- осуществляет контроль наличия в структурном подразделении условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный к ним доступ;
- информирует лиц, осуществляющих обработку персональных данных без использования средств автоматизации, о перечне обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки;
- организует раздельное, т.е. не допускающее смешение, хранение материальных носителей персональных данных (документов, дисков, дискет, USB флеш-накопителей, пр.), обработка которых осуществляется в различных целях.

2.3. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

2.4. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, руководитель структурного подразделения должен обеспечить раздельную обработку персональных данных, исключающую одновременное копирование иных персональных данных, не подлежащих распространению и использованию.

2.5. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, должно производиться способом, исключающим дальнейшую

обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

2.6. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем изготовления нового материального носителя с уточненными персональными данными.

## 3. ПОРЯДОК ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ АВТОМАТИЗАЦИИ

3.1. Обработка персональных данных с использованием средств автоматизации означает совершение действий (операций) с такими данными с помощью объектов вычислительной техники в Корпоративной компьютерной сети Университета (далее - ККС).

Безопасность персональных данных при их обработке в ККС обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, а также используемые в ККС информационные технологии.

3.2. Технические и программные средства защиты информации должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации. Средства защиты информации, применяемые в ККС, в установленном порядке проходят процедуру оценки соответствия.

3.3. Допуск лиц к обработке персональных данных с использованием средств автоматизации осуществляется на основании "Положения о персональных данных работников и обучающихся" (п. 6) при наличии ключей (паролей) доступа.

Работа с персональными данными, содержащимися в ККС, осуществляется в соответствии с «Положением о корпоративной компьютерной сети», «Инструкцией пользователя при работе в корпоративной компьютерной сети», «Инструкцией пользователя при обработке конфиденциальной информации на объектах вычислительной техники», с которыми работник, в должностные обязанности которого входит обработка персональных данных, знакомится под роспись.

3.4. Работа с персональными данными в ККС должна быть организована таким образом, чтобы обеспечивалась сохранность носителей персональных данных и средств защиты информации, а также исключалась возможность неконтролируемого пребывания в этих помещениях посторонних лиц.

3.5. Компьютеры и (или) электронные папки, в которых содержатся файлы с персональными данными, для каждого пользователя должны быть защищены индивидуальными паролями доступа, состоящими из 6 и более символов. Работа на компьютерах с персональными данными без паролей доступа, или под чужими или общими (одинаковыми) паролями, запрещается.

3.6. Пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в том числе Интернет, запрещается.

3.7. При обработке персональных данных в ККС пользователями должно быть обеспечено:

- использование предназначенных для этого разделов (каталогов) носителей информации, встроенных в технические средства, или съемных маркированных носителей;
- недопущение физического воздействия на технические средства

автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

- постоянное использование антивирусного обеспечения для обнаружения зараженных файлов и незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- недопущение несанкционированных выноса из помещений, установки, подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.

3.8. При обработке персональных данных в ККС разработчиками и администраторами систем должны обеспечиваться:

- обучение лиц, использующих средства защиты информации, применяемые в ККС, правилам работы с ними;
- учет лиц, допущенных к работе с персональными данными в ККС, прав и паролей доступа;
- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;
- контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- описание системы защиты персональных данных.

3.9. Специфические требования по защите персональных данных в отдельных автоматизированных системах Школы определяются утвержденными в установленном порядке инструкциями по их использованию и эксплуатации.

## 4. ПОРЯДОК УЧЕТА, ХРАНЕНИЯ И ОБРАЩЕНИЯ СО СЪЕМНЫМИ НОСИТЕЛЯМИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ТВЕРДЫМИ КОПИЯМИ И ИХ УТИЛИЗАЦИИ

4.1. Все находящиеся на хранении и в обращении в Школе съемные носители (диски, дискеты, USB флеш-накопители, пр.), содержащие персональные данные, подлежат учёту. Каждый съемный носитель с записанными на нем персональными данными должен иметь этикетку, на которой указывается его уникальный учетный номер.

4.2. Учет и выдачу съемных носителей персональных данных осуществляет ответственный за обработку персональных данных.

Работники Школы получают учтенный съемный носитель от руководителя подразделения для выполнения работ на конкретный срок.

При получении делаются соответствующие записи в журнале персонального учета съемных носителей персональных данных (далее - журнал учета), который ведется в Школе, осуществляющем работу со съемными носителями персональных данных (Приложение № 2).

По окончании работ пользователь сдает съемный носитель для хранения ответственному, о чем делается соответствующая запись в журнале учета.

4.3. При работе со съемными носителями, содержащими персональные данные, запрещается:

- хранить съемные носители с персональными данными вместе с носителями открытой информации, 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, в гостиницах и т. д.

4.4. При отправке или передаче персональных данных адресатам на съемные носители

записываются только предназначенные адресатам данные. Отправка персональных данных адресатам на съемных носителях осуществляется в порядке, установленном для документов для служебного пользования. Вынос съемных носителей персональных данных для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя структурного подразделения Университета.

4.5. О фактах утраты съемных носителей, содержащих персональные данные, либо разглашения содержащихся в них сведений должно быть немедленно сообщено руководителю соответствующего структурного подразделения Университета и (или) проректору по безопасности.

На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы учета.

4.6. Съемные носители персональных данных, пришедшие в негодность или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с конфиденциальной информацией осуществляется комиссией, созданной приказом ректора Университета.

По результатам уничтожения носителей составляется акт по прилагаемой форме (Приложение № 3).

## 5. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

5.1. С положениями настоящей Инструкции должны быть ознакомлены под роспись все работники Школы и лица, выполняющие работы по договорам и контрактам, имеющие отношение к обработке персональных данных работников, обучающихся Школы и третьих лиц.

С Инструкцией ознакомлены:

| _____ | _____ | _____ |
|---|---|---|
| должность | ФИО | дата |
| _____ | _____ | _____ |
| должность | ФИО | дата |
| _____ | _____ | _____ |
| должность | ФИО | дата |
| _____ | _____ | _____ |
| должность | ФИО | дата |
| _____ | _____ | _____ |
| должность | ФИО | дата |

Приложение 1

**«УТВЕРЖДАЮ»**

_____

руководитель структурного подразделения

«  »_____ 200  г.

**АКТ**

передачи персональных данных третьим лицам

(должность, ФИО)

передал(а) следующие документы, содержащие персональные данные_____:

(ФИО работника, обучающегося)

_____

(перечислить наименования передаваемых документов, содержащих персональные данные)

по запросу_____

(ФИО, должность)

с целью_____

_____.

_____ _____

подпись расшифровка подписи

Документы, содержащие персональные данные принял(а), экземпляр акта получил(а):

_____ _____

подпись расшифровка подписи

«  »_____ 20  г.

Приложение 2

**ЖУРНАЛ**

**учета съемных носителей персональных данных**

_____

наименование структурного подразделения

Начат «__» _____ 200_ г.
Окончен «__» _____ 200_ г.
На _____листах

_____ _____
Должность и ФИО ответственного за хранение Подпись

| № п/п | Метка съемного носителя (учетный номер) | Фамилия пользователя | (Получил, вернул) | Подпись ответственного за хранение съемного носителя | Примечание* |
|---|---|---|---|---|---|
| 1 | | | | | |
| 2 | | | | | |
| 3 | | | | | |
| 4 | | | | | |
| 5 | | | | | |

* Причина и основание окончания использования (№ и дата отправки адресату или распоряжения о передаче, № и дата акта утраты, неисправность, заполнение подлежащими хранению данными)

Приложение 3

**«УТВЕРЖДАЮ»**

_____

«  »_____ 200 г.

**АКТ**

уничтожения съемных носителей персональных данных

Комиссия, наделенная полномочиями приказом ректора ГОУ ВПО СГЭУ от «___»_____ 200_г. № ____ в составе:

(должности, ФИО)

_____

провела отбор съемных носителей персональных данных, не подлежащих дальнейшему хранению:

| № п/п | Дата | Учетный номер съемного носителя | Пояснения |
|---|---|---|---|
| | 2 | 3 | 4 |
| | | | |

Всего съемных носителей_____

(цифрами и прописью)

На съемных носителях уничтожена конфиденциальная информация путем стирания ее на устройстве гарантированного уничтожения информации (механического уничтожения, сжигания и т.п.).

Перечисленные съемные носители уничтожены

_____

путем (разрезания, демонтажа и т.п.),

_____

измельчены и сданы для уничтожения по утилизации вторичного сырья.

Председатель комиссии Подпись Дата

Члены комиссии

(ФИО) Подпись Дата