

Муниципальное общеобразовательное учреждение
«Гимназия №15 Советского района Волгограда»

Утверждено
приказом директора
МОУ гимназии № 15

от _____ № 01-10/518

Директор МОУ гимназии №15
Советского района
Волгограда

Е.Ю. Ляпина



« 20 » 11 2020 г. № 18/20

**Положение об организационно-технических
мерах по сохранности персональных данных
В МОУ гимназии №15**

I. Общие положения.

1.1. Положение об организационно-технических мерах по сохранности персональных данных (далее Положение) в муниципальном общеобразовательном учреждении «Гимназия № 15 Советского района Волгограда» (далее Организация) разработано в соответствии с законодательством Российской Федерации о персональных данных, Трудового кодекса Российской Федерации, Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» с дополнениями и изменениями, в целях обеспечения внутренней защиты персональных данных субъектов.

1.2. Настоящее Положение определяет организационно-технические меры по сохранности персональных данных в Организации, а также устанавливает ответственность лиц, осуществляющих организационно-технические меры по сохранности персональных данных, за невыполнение требований, установленных настоящим Положением.

1.3. Действие настоящего Положения распространяется на всех работников Организации, осуществляющих организационно-технические меры по сохранности персональных данных в Организации.

1.4. В организации приказом директора назначается лица, ответственные по организационно-техническим мерам по защите персональных данных субъектов на электронных носителях и на бумажных (неэлектронных) носителях.

II. Организационно-технические меры по защите персональных данных субъектов на электронных носителях.

2.1. Ответственный по организационно-техническим мерам по защите персональных данных субъектов на электронных носителях в Организации (далее - ответственный за электронные данные) должен применять следующие меры по защите персональных данных субъектов на электронных носителях:

2.1.1. защищать все ПК, на которых находится информация с персональными данными, паролями. Пароль к доступу этих ПК сообщается только тем работникам, которые по приказу директора Организации имеют доступ к персональным данным;

2.1.2. для предотвращения потери данных информационных систем в случае сбоя, использовать систему резервного копирования;

2.1.3. при передаче по внутренней локальной сети (далее ВС) необходимо ограничить количество компьютеров с возможностью копирования файлов и применения флэш-накопителей;

2.1.4. уточнять в установленном порядке обязанности пользователей ВС по поддержанию уровня защиты ВС;

2.1.5. анализировать данные журнала учёта работы ВС с целью выявления возможных нарушений требований защиты;

2.1.6. обеспечить доступ к защищаемой информации пользователям ВС согласно их правам доступа при получении оформленного соответствующим образом разрешения;

2.1.7. запрещать и немедленно блокировать попытки изменения программно-аппаратной среды ВС без согласия порядка ввода новых (отрегламентированных) технических и программных средств и средств защиты;

2.1.8. запрещать и немедленно блокировать применение пользователям ВС программ, с помощью которых возможны факты несанкционированного доступа к ресурсам ВС;

2.1.9. незамедлительно докладывать руководству обо всех попытках нарушения защиты ВС и базы данных;

2.1.10. контролировать правильность применения пользователями ВС средств защиты;

2.1.11. не допускать установку, использование, хранение и размножение в ВС программных средств, не связанных с выполнением функциональных задач.

III. Организационно-технические меры по защите персональных данных субъектов на бумажных носителях.

3.1. Ответственный по организационно-техническим мерам по защите персональных данных субъектов на бумажных носителях (далее ответственный за неэлектронные данные) должен применять следующие меры по защите персональных данных субъектов на электронных носителях:

- 3.1.1.определить место хранения персональных данных (сейф, либо другие места хранения данных, к которым нет общего доступа);
- 3.1.2.ограничить круг лиц, имеющих доступ к персональным данным в соответствии с приказом директора Организации;
- 3.1.3.соблюдать условия, обеспечивающие сохранность персональных данных (не оставлять открытым сейф и другие места хранения документов; не оставлять классные журналы, личные дела и другие документы с персональными данными на столах после завершения работы с ними);
- 3.1.4.документы, содержащие персональные данные субъектов, хранить в недоступном для посторонних лиц месте;
- 3.1.5.использовать персональные данные субъекта, полученные только от него лично и с его письменного согласия;
- 3.1.6.соблюдать требование конфиденциальности персональных данных субъектов;
- 3.1.7.исключать или исправлять по письменному требованию субъекта недостоверные или неполные персональные данные субъекта, а также данные с нарушением требований законодательства РФ;
- 3.1.8.не запрашивать информацию о состоянии здоровья субъектов, за исключением случаев предусмотренных законом;
- 3.1.9.обеспечить субъекту свободный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные субъекта.

IV. Ответственность за нарушение организационно-технических мер по защите персональных данных субъектов.

- 4.1.Работникам, ответственным за организационно-технические меры по защите персональных данных субъектов на электронных носителях запрещается: оставлять свое рабочее место без контроля, в том числе в рабочем состоянии; фиксировать учётные данные пользователя (пароли, идентификаторы, ключи и др.) на твёрдых носителях, а также передавать их посторонним лицам.
- 4.2.Работники, ответственные за организационно-технические меры по защите персональных данных субъектов несут ответственность в соответствии с действующим законодательством за неисполнение или недобросовестное исполнение настоящего Положения.

V. Права ответственных лиц за организационно-технические меры по защите персональных данных субъектов.

- 5.1.Работник имеет право:
- 5.1.1.Получать доступ к своим персональным данным и ознакомление с ними, включая право на безвозмездное получение копий любой записи, содержащей персональные данные Работника;
- 5.1.2.Требовать от работодателя уточнения, исключения или исправления неполных, неверных, устаревших, недостоверных, незаконно полученных или не являющихся необходимыми для работодателя персональных данных;
- 5.1.3.Получать от работодателя:
- сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
 - сроки обработки персональных данных, в том числе сроки их хранения;

6. Порядок ввода в действие и внесение изменений в настоящее Положение.

- 6.1.Настоящее Положение вступает в силу с момента утверждения его директором Организации и действует в течение пяти лет или до момента внесения изменений.
- 6.2.Изменения в настоящее Положение вносятся приказом директора Организации.