УТВЕРЖДЕНА
приказом директора
ГКОУ АО «Школа-интернат №1»
от 01.09.2026 № 173

ИНСТРУКЦИЯ
по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

1. Общие положения

1.1. Инструкция определяет порядок обеспечения безопасности персональных данных (ПДн) при их обработке в информационных системах персональных данных (ИСПДн) [наименование школы-интерната].

1.2. Требования Инструкции обязательны для всех работников, допущенных к обработке ПДн, а также для подрядчиков, привлекаемых к эксплуатации ИСПДн.

1.3. Инструкция разработана в соответствии с:

- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- методическими документами ФСТЭК России по защите информации.

2. Термины и определения

Используемые термины применяются в значениях, установленных законодательством РФ о персональных данных.

3. Организационные меры безопасности

3.1. Доступ к ПДн предоставляется только работникам, включённым в утверждённый приказом директора перечень должностей, допущенных к обработке ПДн.

3.2. Назначение ответственного за организацию обработки ПДн и ответственного за обеспечение безопасности ПДн оформляется приказом директора.

3.3. Все работники, допущенные к ПДн, обязаны пройти инструктаж и подписать обязательство о неразглашении ПДн.

3.4. В трудовых договорах (должностных инструкциях) закреплены обязанности по обеспечению конфиденциальности ПДн и ответственность за их нарушение.

4. Технические меры защиты

4.1. ИСПДн должны обеспечивать:

- идентификацию и аутентификацию пользователей;
- разграничение прав доступа по ролям;

- регистрацию событий безопасности (журналирование);
- антивирусную защиту и контроль целостности ПО;
- резервное копирование данных и восстановление при инцидентах.

4.2. Использование средств защиты информации (СЗИ) осуществляется в соответствии с эксплуатационной документацией и требованиями регуляторов.

4.3. На рабочих местах запрещается:

- установка нелицензионного и неучтённого ПО;
- подключение личных мобильных устройств и съёмных носителей без согласования;
- передача учётных данных третьим лицам.

5. Порядок работы пользователей с ПДн

5.1. Пользователь обязан:

- использовать только свою учётную запись и надёжный пароль;
- блокировать экран АРМ при отлучении от рабочего места;
- не оставлять распечатки с ПДн на столе или в принтере;
- не пересылать ПДн по незащищённым каналам связи (обычная почта, мессенджеры).

5.2. При обнаружении признаков инцидента (вирус, утечка, подозрительная активность) пользователь обязан немедленно сообщить ответственному за безопасность ПДн.

6. Контроль и аудит

6.1. Не реже 1 раза в квартал проводится внутренний контроль выполнения требований по защите ПДн.

6.2. Результаты контроля оформляются актом, при выявлении нарушений - разрабатывается план корректирующих мероприятий.

6.3. Периодичность оценки угроз и актуализации модели угроз - не реже 1 раза в год либо при существенных изменениях в ИТ-инфраструктуре.

7. Хранение и уничтожение носителей

7.1. Бумажные носители с ПДн хранятся в запираемых шкафах/сейфах.

7.2. Электронные носители (флешки, диски) подлежат учёту в журнале и уничтожению с гарантированным стиранием данных.

7.3. Уничтожение ПДн производится по акту в сроки, установленные законодательством и локальными актами.

8. Ответственность

8.1. За нарушение требований Инструкции работники несут дисциплинарную, материальную, административную и иную ответственность в соответствии с законодательством РФ.