СОГЛАСОВАНО
Профсоюзный комитет
МАОУ СОШ № 103
Протокол от 15.08.25 № 43
Председатель профкома
_____/Салтыкова Е.В.
М.П.

ПРИНЯТО
решением общего собрания
трудового коллектива
МАОУ СОШ № 103
протокол № 2 от 28.08.2025

УТВЕРЖДЕНО
приказ № 1098 - О от 01.09.2025
Директор _____ С.Ф.Чернявская
«01» сентября 2025 г.

ПОЛОЖЕНИЕ
о защите персональных данных в МАОУ СОШ №103

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (в редакции Федерального закона от 24.06.2025 № 156-ФЗ), Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»; Приказом Роскомнадзора от 19.06.2025 № 140 «Об утверждении требований к обезличиванию персональных данных».

1.2. Положение определяет систему организационных и технических мер, направленных на обеспечение безопасности персональных данных (далее - ПДн) при их обработке в МАОУ СОШ №103 (далее - Оператор, Школа).

1.3. **Цель Положения** - предотвращение несанкционированного доступа, уничтожения, модификации, блокирования, копирования, распространения персональных данных, а также иных неправомерных действий.

2. Угрозы безопасности персональных данных

2.1. Оператор исходит из того, что основными угрозами безопасности ПДн являются:

- несанкционированный доступ со стороны посторонних лиц;
- неправомерные действия работников Школы, допущенных к обработке ПДн;
- перехват данных при передаче по каналам связи;
- случайное уничтожение или искажение данных;
- утрата бумажных носителей;
- вредоносные программы (вирусы);
- атаки на информационные системы;
- утечки через технические каналы.

3. Классификация информационных систем персональных данных (ИСПДн)

3.1. В Школе функционируют следующие ИСПДн:

- **ИСПДн-1** - кадровая система (1С: Предприятие, АИС Сетевой город. Образование) - обрабатываются ПДн работников;
- **ИСПДн-2** - бухгалтерская система - 1С: Предприятие, Контур-экстерн, ПДн работников (для начисления зарплаты);
- **ИСПДн-3** - система учета контингента (ФИС ФРДО, РБД ГИА-9, РБД ГИА-11, АИС Е-услуги, АИС Сетевой город. Образование) - ПДн обучающихся;
- **ИСПДн-4** - электронный журнал (АИС Сетевой город. Образование) - ПДн обучающихся и родителей;
- **ИСПДн-5** - сайт Школы - ПДн пользователей (обращения, заявки).

3.2. Для каждой ИСПДн определен класс защищенности.

4. Организационные меры защиты персональных данных

4.1. **Назначение ответственных лиц:**

- Приказом директора назначено лицо, ответственное за организацию обработки и защиты ПДн.
- Приказом директора утвержден перечень должностей, допущенных к обработке ПДн.

4.2. **Документационное обеспечение:**

- Положение о порядке обработки, хранения, использования и уничтожения персональных данных работников, обучающихся и их родителей (законных представителей);
- Настоящее Положение о защите персональных данных;
- Инструкция пользователя информационной системы;
- Политика об обработке ПДн
- Журнал учета обращений субъектов ПДн;
- Журнал учета инцидентов;
- Журнал выдачи паролей;
- Формы согласий на обработку ПДн (отдельные документы);
- Форма обязательства о неразглашении ПДн.

4.3. **Допуск работников к обработке ПДн:**

- Работники допускаются к обработке ПДн только после подписания Обязательства о неразглашении.
- Работники проходят инструктаж по вопросам защиты ПДн.
- Работники знакомятся с локальными актами под роспись.

4.4. **Внутренний контроль:**

- Не реже одного раза в полугодие проводится проверка соблюдения требований защиты ПДн.
- По результатам проверок составляются акты (протоколы), при необходимости — планы устранения нарушений.

5. Технические меры защиты персональных данных

5.1. **Разграничение доступа:**

- Доступ к ИСПДн осуществляется только после прохождения аутентификации (логин/пароль).
- Пароли должны соответствовать требованиям сложности (не менее 8 символов, буквы разного регистра, цифры).

- Пароли подлежат смене не реже одного раза в 90 дней.
- Запрещается использование групповых учетных записей.

5.2. **Антивирусная защита:**

- На всех рабочих станциях и серверах, где обрабатываются ПДн, установлено антивирусное программное обеспечение с регулярным обновлением баз.

5.3. **Межсетевое экранирование:**

- Обеспечена защита периметра сети, ограничен доступ из внешних сетей к внутренним ресурсам с ПДн.

5.4. **Регистрация и учет:**

- В ИСПДн ведется регистрация действий пользователей (логирование).
- Срок хранения логов — не менее 1 года.

5.5. **Резервное копирование:**

- Осуществляется регулярное резервное копирование баз данных, содержащих ПДн.
- Резервные копии хранятся в защищенном месте.

5.6. **Защита при передаче:**

- При передаче ПДн по открытым каналам связи (например, через Интернет) используется шифрование.

6. Обезличивание персональных данных

6.1. В случаях, когда для статистических, аналитических или иных целей не требуется идентификация конкретного лица, Оператор проводит **обезличивание персональных данных**.

6.2. Обезличивание осуществляется в соответствии с требованиями Приказа Роскомнадзора от 19.06.2025 № 140.

6.3. Ответственный за обработку ПДн контролирует, чтобы при подготовке отчетов (например, для внутреннего анализа успеваемости, статистических справок) использовались только обезличенные данные.

7. Действия при инцидентах (нарушениях безопасности)

7.1. При обнаружении фактов несанкционированного доступа, утери документов, компрометации паролей работник обязан немедленно сообщить ответственному за ПДн и системному администратору.

7.2. **Порядок действий при инциденте:**

1. Немедленная блокировка доступа (отключение, смена паролей).
2. Оценка масштабов инцидента.
3. Служебное расследование (создание комиссии).
4. Принятие мер по устранению последствий.
5. Информирование Роскомнадзора (в случаях, предусмотренных законом.

7.3. По каждому инциденту составляется акт, принимаются меры дисциплинарного характера к виновным лицам.

8. Контроль доступа в помещения

8.1. Помещения, где осуществляется обработка ПДн (архив, отдел кадров, приемная директора, бухгалтерия, серверная, кабинет для работы с базой ФИС ФРДО), должны быть оборудованы замками, исключающими бесконтрольный вход посторонних лиц.

8.2. В нерабочее время помещения закрываются, сдаются под охрану (или опечатываются (кабинет ФИС ФРДО)).
8.3. Документы, содержащие ПДн, не должны оставляться на рабочих столах в отсутствие сотрудников.

9. Ответственность за нарушение требований защиты

9.1. Лица, виновные в нарушении требований настоящего Положения, привлекаются к дисциплинарной, административной или уголовной ответственности в соответствии с законодательством РФ.
9.2. Работник, допустивший утерю документа (носителя), содержащего ПДн, обязан возместить Оператору убытки (в порядке, установленном трудовым законодательством).

10. Заключительные положения

10.1. Настоящее Положение вступает в силу с даты его утверждения директором.
10.2. Все изменения и дополнения в Положение вносятся путем утверждения новой редакции.
10.3. С настоящим Положением должны быть ознакомлены под роспись все работники, допущенные к обработке персональных данных.