УТВЕРЖДЕНО
Директор МАОУ СОШ № 96
_____/ Подносова Т.Б.
«___» _____ 202

Подписано цифровой подписью: Подносова Татьяна Борисовна
DN: E=uc_fk@roskazna.ru, S=77 Москва, ИНН ЮЛ=7710568760, ОГРН=1047797019830, STREET="Большой Златоустинский переулок, д. 6, строение 1", L=г. Москва, C=RU, O=Федеральное казначейство, CN=Федеральное казначейство
Причина: Я являюсь автором этого документа
Дата: 12 Март 2026 г. 11:35:40

ПОЛОЖЕНИЕ
о защите персональных данных работников и иных субъектов (мерах по обеспечению безопасности персональных данных при их обработке)

1. Общие положения

1.1. Настоящее Положение о защите персональных данных (далее — Положение) разработано в соответствии с Трудовым кодексом РФ, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства РФ от 01.11.2012 № 1119 (об утверждении требований к защите данных в информационных системах), а также иными нормативными актами в области защиты информации.

1.2. Положение устанавливает единую систему защиты конфиденциальности персональных данных, обрабатываемых в МАОУ СОШ № 96 (далее — Оператор), определяет порядок обеспечения безопасности данных при их сборе, хранении, передаче и уничтожении.

1.3. Целью Положения является предотвращение утечек, неправомерного или случайного доступа к персональным данным, их уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также иных неправомерных действий.

1.4. Требования настоящего Положения обязательны для исполнения всеми работниками Оператора, допущенными к обработке персональных данных.

2. Организация системы защиты персональных данных

2.1. Ответственность за организацию защиты персональных данных возлагается на **ответственного за организацию обработки персональных данных**, назначаемого приказом руководителя.

2.2. В Операторе действует разрешительная система доступа работников к персональным данным:

- Каждый работник имеет доступ только к тем данным, которые необходимы ему для выполнения конкретных должностных обязанностей.
- Перечень лиц, имеющих доступ к персональным данным, утверждается руководителем.

2.3. Работники, допущенные к обработке персональных данных, обязаны подписать **Обязательство о неразглашении персональных данных**. Без подписания такого обязательства работник не допускается к работе с данными.

3. Меры по обеспечению безопасности персональных данных

3.1. Для обеспечения безопасности персональных данных Оператором применяется комплекс правовых, организационных и технических мер.

3.2. **Организационные и правовые меры:**

- Разработка и утверждение локальных актов по обработке и защите персональных данных.
- Ознакомление работников с данными актами под роспись.
- Определение мест хранения материальных носителей персональных данных (сейфы, металлические шкафы, помещения с ограниченным доступом).
- Регламентация порядка уничтожения документов и носителей (с обязательным составлением акта комиссией).

3.3. **Технические меры защиты (для автоматизированных систем):**

- **Идентификация и аутентификация:** Присвоение каждому работнику уникального логина и пароля для входа в информационную систему. Пароли должны соответствовать требованиям сложности (не менее 8 символов, буквы в разных регистрах, цифры) и регулярно меняться.
- **Антивирусная защита:** Обязательное использование лицензионного антивирусного программного обеспечения на всех рабочих станциях и серверах, где обрабатываются персональные данные.
- **Межсетевое экранирование:** Обеспечение защиты локальных сетей Оператора при подключении к сети Интернет.
- **Регистрация и учет:** Ведение электронных журналов (логов) доступа к базам данных, позволяющих определить, кто, когда и с какой целью обращался к персональным данным.
- **Резервирование:** Регулярное создание резервных копий баз данных для возможности восстановления информации в случае сбоев.

3.4. **Меры защиты при обработке на бумажных носителях:**

- Документы, содержащие персональные данные, хранятся в запираемых шкафах (сейфах), исключающих доступ посторонних лиц.
- При выходе из кабинета в нерабочее время работник обязан убирать документы в шкаф и опечатывать его (при необходимости).
- Запрещается оставлять документы с персональными данными на рабочих столах без присмотра.

4. Правила обработки и конфиденциальность

4.1. Работникам, имеющим доступ к персональным данным, запрещается:

- Сообщать персональные данные работника или иного субъекта третьей стороне без письменного согласия субъекта (за исключением случаев, предусмотренных федеральным законом).
- Передавать персональные данные в коммерческих целях без согласия субъекта.

- Разглашать персональные данные по телефону или в мессенджерах (например, отправлять фотографии паспортов, списки сотрудников в открытые чаты).
- Оставлять без контроля электронные носители (флешки, диски) с персональными данными.

4.2. При передаче персональных данных внутри организации (между отделами) допускается передача только тех сведений, которые необходимы для выполнения конкретной работы (принцип минимизации).

4.3. **Обработка данных родственников:**

- Обработка данных членов семьи сотрудника (например, для заполнения личной карточки Т-2, выплаты пособий) допускается в объеме, строго необходимом для исполнения законодательства.
- Для сбора контактных данных родственников (номера телефонов для экстренной связи) рекомендуется получить письменное согласие самого родственника. Альтернативой может служить письменное заявление сотрудника о том, что он гарантирует наличие согласия от родственника на передачу данных.

4.4. **Данные на интернет-сайтах:**

- Публикация персональных данных (фотографий, ФИО, должностей) на официальном сайте или в соцсетях организации допускается только при наличии отдельного **согласия на распространение персональных данных**.
- Такое согласие должно быть конкретным: содержать цель распространения, перечень данных, срок действия и способы отзыва.

5. Обязанности работников по защите персональных данных

5.1. Работник, допущенный к обработке персональных данных, обязан:

- Строго соблюдать требования настоящего Положения и законодательства РФ.
- Немедленно сообщать своему непосредственному руководителю о фактах утраты документов (носителей), содержащих персональные данные, а также о попытках несанкционированного доступа к ним.
- Не допускать использования персональных данных в корыстных целях.
- В случае увольнения передать все имеющиеся у него документы и носители с персональными данными ответственному лицу или руководителю.

6. Ответственность за нарушение норм защиты

6.1. Лица, виновные в нарушении порядка обращения с персональными данными (разглашение, утеря, несанкционированный доступ), несут ответственность в соответствии с действующим законодательством РФ.

6.2. Виды ответственности:

- **Дисциплинарная:** замечание, выговор, увольнение (за разглашение охраняемой законом тайны).

- **Административная:** штрафы по ст. 13.11, 13.14 КоАП РФ (для должностных лиц — до 200 000 рублей, для юридических лиц — до 300 000 рублей).
- **Уголовная:** по ст. 137 УК РФ (за нарушение неприкосновенности частной жизни).

7. Заключительные положения

7.1. Настоящее Положение вступает в силу с даты его утверждения руководителем организации и действует до его отмены или замены новым.

7.2. Все изменения и дополнения в Положение утверждаются руководителем организации.

7.3. Работники организации должны быть ознакомлены с настоящим Положением под подпись