УТВЕРЖДЕНО
приказом директора
МАОУ «СОШ № 10» г. Кунгура
от 09.11.2026 № 290/1

ПАМЯТКА

работнику по профилактике нарушений в сфере персональных данных

Настоящая памятка разработана в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (с учётом изменений, вступивших в силу в 2024–2026 годах), письмом Министерства информационного развития и связи Пермского края от 17.09.2026 № 20-01-10-1322 и локальными актами школы. Памятка обязательна для всех работников МАОУ «СОШ №10».

1. Помните: персональные данные — под особой охраной

- Персональные данные — любые сведения о работнике, обучающемся (воспитаннике) или родителе (законном представителе): Ф. И. О., дата рождения, адрес, телефоны, сведения об успеваемости, состоянии здоровья, семейном положении, фотографиях и др.
- Обрабатывайте персональные данные только в объёме, необходимом для исполнения трудовых обязанностей, и только на законных основаниях (согласие субъекта, договор, закон).
- Не разглашайте персональные данные третьим лицам без согласия субъекта и поручения работодателя.

2. Мессенджеры и групповые чаты

- **Не размещайте в чатах персональные данные** (Ф. И. О., телефоны, адреса, сведения об успеваемости, здоровье, семейном положении), если они не связаны с целью создания чата.
- **Не передавайте в чатах логины и пароли** от учётных записей информационных систем (в том числе образовательных сервисов) и аккаунтов социальных сетей.
- **Не пересылайте файлы с персональными данными** (списки классов, таблицы с контактами, скриншоты) в личные сообщения, личные аккаунты и облачные хранилища.
- **Вступайте в рабочие и классные чаты только по приглашению администратора.**
- **Администратор чата:** разрабатывает правила общения в чате; исключает уволившихся сотрудников из корпоративных чатов, а родителей выбывших детей — из чатов класса (группы); не передаёт право управления участниками иными лицами; незамедлительно удаляет или блокирует сторонние ссылки, присланные в чат.

- **Участник чата:** при получении подозрительной ссылки, файла или сообщения от чужого имени — не открывать их и сообщить администратору чата и ответственному за защиту персональных данных.

3. Служебные компьютеры и рабочее место

- Не храните на служебных компьютерах личную информацию и личные документы, не используйте их в целях, не связанных с исполнением трудовых обязанностей.
- Не сохраняйте документы с персональными данными на личные носители (флеш-карты, личные телефоны) и в облачные хранилища.
- Блокируйте компьютер (Windows + L), когда отходите от рабочего места, даже на короткое время.
- Не оставляйте документы с персональными данными на столе в доступном для посторонних виде; бумажные носители храните в закрытых шкафах/сейфах.
- Не сообщайте свои пароли никому, включая коллег и руководителей; при подозрении на компрометацию пароля немедленно сообщите ответственному за защиту персональных данных.

4. Совещания, демонстрации, публикация в сети «Интернет»

- Перед демонстрацией документа на экране (совещание, заседание, открытый урок) убедитесь в отсутствии в нём посторонних персональных данных.
- Перед выгрузкой документов в информационные системы проверьте, что персональные данные не попадут в открытый контур (общедоступные поля, автоматическая публикация приложений к документам).
- Публикуйте на сайте и публичных страницах школы только ту информацию об обучающихся, которая разрешена действующим законодательством и согласием родителей (законных представителей).

5. Электронная почта и документооборот

- Перед отправкой письма с вложением проверьте адрес получателя: из-за схожести символов (l/I/1, o/a) легко ошибиться и направить персональные данные посторонним.
- При рассылке нескольким получателям используйте скрытую копию (BCC) или обезличенные списки.
- Не направляйте персональные данные в мессенджеры и на личные адреса электронной почты.

6. Права субъектов персональных данных

- На запрос субъекта о его персональных данных (уточнение, блокирование, уничтожение) — не отвечайте самостоятельно: передайте обращение ответственному за защиту персональных данных или директору.

- Уведомите ответственного о любой ошибке: сообщение о неверных данных, случайная рассылка, утеря документа.

7. При инциденте — действуйте немедленно

- **Сообщите** руководителю и ответственному за защиту персональных данных в тот же день об утечке, ошибочной рассылке, взломе аккаунта, утере носителя.
- **Не скрывайте** инцидент и не пытайтесь «уладить» его самостоятельно.
- **Помните:** с 30.05.2025 уведомление Роскомнадзора об инциденте обязательно в течение 24 часов, а ответственность за утечки персональных данных (ст. 13.11 КоАП РФ) предусматривает оборотные штрафы для организаций — до 3 % годовой выручки при повторной утечке.