

**Муниципальное бюджетное общеобразовательное учреждение
Полевского муниципального округа Свердловской области**

**«Средняя общеобразовательная школа
№18»**

УТВЕРЖДАЮ: _____ Т.Г.
Тарасова, директор
муниципального бюджетного
общеобразовательного учреждения
Полевского муниципального округа
Свердловской области «Средняя
общеобразовательная школа № 18»

Приказ от 12.01.2026 г № 02-Д

ПОЛОЖЕНИЕ

**о порядке действий при инциденте (утечке персональных данных)
муниципального бюджетного общеобразовательного учреждения
Полевского муниципального округа Свердловской области
«Средняя общеобразовательная школа №18»**

1. Общие положения

1.1. Настоящий Порядок определяет действия работников муниципального бюджетного общеобразовательного учреждения Полевского муниципального округа Свердловской области «Средняя общеобразовательная школа №18» при выявлении инцидента, связанного с неправомерной или случайной передачей (предоставлением, распространением, доступом) персональных данных, повлёкшей нарушение прав субъектов персональных данных.

1.2. Инцидентом признаётся в том числе: утрата материального носителя (флеш-накопитель, папка, журнал); направление документа с персональными данными не тому адресату; размещение сведений в открытом доступе без законного основания; доступ к информационной системе под чужой учётной записью; хищение техники, содержащей персональные данные; иные события, повлёкшие или способные повлечь нарушение прав субъектов персональных данных.

1.2а. Сроки уведомления, установленные разделами 3 и 4 настоящего Порядка, исчисляются с момента выявления инцидента — независимо от того, кем он выявлен: самим Оператором, уполномоченным органом по защите прав субъектов персональных данных либо иным заинтересованным лицом (в том числе при внешнем сообщении). Момент внутреннего доклада директору начало срока не переносит.

1.3. Ответственный за организацию обработки персональных данных — Шустова Ирина Эдуардовна, заместитель директора по УВР], телефон 8 (343 50) 45618 (многоканальный), резервный контакт (замещает ответственного при его недоступности, включая полномочия на подписание и направление уведомлений) — Антипова Юлия Александровна, заместитель директора по АХР, телефон 8 (34350) 45618 (многоканальный).

2. Действия работника, обнаружившего инцидент

2.1. Немедленно, независимо от времени суток, сообщить ответственному за организацию обработки персональных данных по телефону 8 (34350) 45618; при недоступности —

директору.

2.2. По возможности прекратить дальнейшее распространение сведений (отозвать письмо, закрыть доступ, изъять носитель), не удаляя при этом следы события: журналы, переписку, снимки экрана.

2.3. В течение трёх часов с момента обнаружения оформить служебную записку с описанием обстоятельств: что произошло, когда обнаружено, какие сведения затронуты, кто мог получить доступ.

3. Действия в первые 24 часа

3.1. Ответственный за организацию обработки персональных данных:

1) фиксирует дату и время выявления инцидента (пункт 1.2а) в журнале учёта инцидентов, связанных с персональными данными;

2) оценивает, какие категории субъектов и какие данные затронуты, предполагаемое число записей;

3) заполняет и направляет уведомление уполномоченному органу по защите прав субъектов персональных данных через специализированный раздел на его официальном сайте (личный кабинет оператора персональных данных) либо, при отсутствии доступа к нему, на бумажном носителе по почтовому адресу этого органа, — в течение 24 часов с момента выявления инцидента, сохраняя подтверждение направления (номер уведомления, почтовую квитанцию);

4) докладывает директору.

3.2. В уведомлении указываются: реквизиты Оператора (наименование, ИНН, адрес, адрес электронной почты); дата и время выявления инцидента; характеристика затронутых персональных данных и предполагаемое число субъектов; предполагаемые причины инцидента; предполагаемый вред правам субъектов персональных данных; принятые меры по устранению последствий; сведения о лице, уполномоченном на взаимодействие по вопросам инцидента (как правило — ответственный за организацию обработки персональных данных либо его резервный контакт по пункту 1.3, с указанием контактов).

3.3. Директор принимает решение о мерах по ограничению последствий: блокирование доступа, смена паролей, изъятие носителей, обращение в правоохранительные органы (при признаках преступления).

3.4. Если уполномоченный орган запрашивает дополнительные сведения к ранее направленному уведомлению, ответственный за организацию обработки персональных данных обеспечивает ответ в течение трёх рабочих дней с момента получения запроса, а на требование о представлении сведений о результатах расследования, если они ещё не поступили, — в течение одного рабочего дня; данные сроки не заменяют и не продлевают срок направления уведомления за 72 часа по разделу 4 настоящего Порядка.

3.5. Если инцидент связан с компьютерной атакой или иным компьютерным инцидентом в информационной системе Оператора (в том числе обслуживаемой внешним ИТ-подрядчиком), ответственный за организацию обработки персональных данных дополнительно определяет применимую категорию Оператора по приказу ФСБ России от 13.02.2023 № 77: при организованном взаимодействии с Национальным координационным центром по компьютерным инцидентам (НКЦКИ) — направляет информацию по установленным для этого канала; в остальных случаях — использует те же специализированные уведомления уполномоченного органа по защите прав субъектов персональных данных, что и по пункту 3.1. На запрос НКЦКИ о результатах проверки Оператор отвечает в течение 24 часов с момента его получения. Наличие договора с внешним ИТ-подрядчиком не переносит на него обязанность Оператора направить уведомление в установленный срок; отдельное дублирующее письмо в ФСБ России настоящим Порядком не предусматривается и не требуется, если категория Оператора не предполагает такого канала.

4. Внутреннее расследование и уведомление в 72 часа

4.1. Приказом директора создаётся комиссия по расследованию инцидента в составе не менее трёх работников.

4.2. Комиссия устанавливает: причины инцидента; перечень затронутых персональных данных и субъектов; лиц, действия которых стали причиной инцидента; достаточность принятых мер.

4.3. Результаты оформляются актом внутреннего расследования, в том числе, если по итогам расследования факт неправомерной или случайной передачи персональных данных не подтвердился (сообщение поступило от внешнего лица, принадлежность базы данных Оператору не установлена либо распространение относится к ранее уже сообщённому инциденту).

4.4. Ответственный за организацию обработки персональных данных направляет в уполномоченный орган уведомление о результатах внутреннего расследования — в течение 72 часов с момента выявления инцидента (пункт 1.2а). Если за 72 часа установить виновных лиц не удалось, уведомление направляется с результатами расследования на текущий момент с указанием, что установление лиц продолжается; это не основание задерживать уведомление. Если по итогам расследования факт инцидента не подтвердился, уведомление за 72 часа направляется с приложением акта внутреннего расследования, подтверждающего отсутствие факта неправомерной или случайной передачи персональных данных, — сомнение в достоверности первичного сообщения не освобождает от направления уведомления в установленный срок.

5. После завершения расследования

5.1. По решению директора принимаются меры: изменение порядка работы, дополнительное обучение работников, пересмотр прав доступа, привлечение работника к дисциплинарной ответственности (в порядке статей 192 и 193 Трудового кодекса Российской Федерации, при наличии оснований).

5.2. Вопрос об информировании субъектов персональных данных решается директором с учётом характера инцидента и требований законодательства, не позднее пяти рабочих дней, с даты завершения внутреннего расследования. Если инцидент создаёт продолжающийся риск для субъектов (например, скомпрометированный пароль ещё действует, утраченный носитель не найден), срочное предупреждение затронутых субъектов не откладывается до завершения расследования и направляется незамедлительно после выявления такого риска — независимо от срока пункта 5.2, который применяется к решению об информировании по общим результатам расследования.

5.3. Материалы инцидента (служебные записки, акт, копии уведомлений) хранятся у ответственного за организацию обработки персональных данных по сроку.

6. Заключительные положения

6.1. Все работники знакомятся с настоящим Положением под подпись при приёме на работу.

6.2. Порядок пересматривается при изменении законодательства о персональных данных либо по итогам расследования, выявившего пробел в самом порядке действий.

6.3. Действующая редакция Положения хранится весь срок её действия.

6.4. Изменения в Положение утверждаются приказом директора. Работники знакомятся с новой редакцией или изменениями под подпись до начала их применения.