

ОБСУЖДЕНО
на заседании
педагогического совета
Протокол от 25 июня 2021 г. № 23

УТВЕРЖДАЮ:
Директор МБОУ «СОШ № 31»
Л.О. Маликова
Приказ от 20 июля 2021 г. № 337-о

ПОРЯДОК УНИЧТОЖЕНИЯ, БЛОКИРОВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ В МУНИЦИПАЛЬНОМ БЮДЖЕТНОМ ОБЩЕОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ «СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 31»

I. Общие положения

1.1. Настоящий Порядок определяет условия и способы:

- уничтожения бумажных носителей (документов), содержащих персональные данные по достижению цели обработки персональных данных;
- персональные данные в машинных носителях информации, в том числе персональных данных, и при необходимости самих машинных носителей информации.

II. Блокирование и уничтожение персональных данных, содержащихся в машинных носителях информации

2.1. Блокирование информации, содержащей персональные данные субъекта персональных данных, производится в случаях:

- если ПД являются неполными, устаревшими, недостоверными;
- если сведения незаконно полученными или не являются необходимыми для заявленной оператором персональных данных цели обработки.

2.2. В случае подтверждения факта недостоверности ПД уполномоченное оператором лицо на основании документов, представленных субъектом ПД, уполномоченным органом по защите прав субъектов ПД или полученных в ходе самостоятельной проверки, обязано уточнить персональные данные и снять их блокирование.

2.3. В случае выявления неправомерных действий с ПД уполномоченное оператором лицо обязано устранить (организовать устранение) допущенные нарушения. В случае невозможности устранения допущенных нарушений необходимо в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с ПД, уничтожить ПД.

2.4. Об устранении допущенных нарушений или об уничтожении ПД уполномоченное оператором лицо обязано уведомить субъекта ПД, а в случае если обращение или запрос были направлены уполномоченным органом по защите прав субъектов ПД, также указанный орган.

2.5. Уполномоченное оператором лицо обязано уничтожить персональные данные субъекта ПД в случаях:

- достижения цели обработки ПД оператора;
- отзыва субъектом согласия на обработку своих ПД.

2.6. Уничтожение ПД должно быть осуществлено в течение трех дней с указанных моментов. В согласии субъекта ПД на обработку его персональных данных могут быть установлены иные сроки уничтожения ПД. Уполномоченное оператором лицо (например, руководитель службы информационной безопасности) должно направить уведомление о факте уничтожения персональных данных.

III. Работа с бумажными носителями (документами)

3.1. Виды и периоды уничтожения бумажных носителей, содержащих персональные данные представлены в Таблице №1.

Таблица № 1. Виды и периоды уничтожения бумажных носителей, содержащих ПД

№ п/п	Документ	Срок хранения	Действия при окончании срока хранения
1	Документы (сведения, содержащие ПД о работниках Оператора), переданные и сформированные при трудоустройстве работника	75 лет	Уничтожение
2	Документы об обучающихся (сведения, содержащие ПД обучающихся)	Установленные для данных документов сроки хранения	Уничтожение
3	Другие документы с грифом «Конфиденциально» и «для служебного пользования» (журналы учета, списки доступа, эксплуатационная документация и т.д.)	Хранятся до замены на новые, если не указан конкретный срок	Уничтожение

3.2. Документы, указанные в п. 3.1. должны находиться в сейфах, печатаемых печатями сотрудника отдела кадров или учебной части. Исключение составляют документы, обрабатываемые в настоящий момент на рабочем месте.

3.3. По окончании срока хранения документы, указанные в п.3.1., уничтожаются путем измельчения на мелкие части (или иным способом), исключающие возможность последующего восстановлению информации или сжигаются.

IV. Работа с машинными носителями информации

4.1. Виды и периоды уничтожения ПД, хранимых в электронном виде («файлах») на жестком диске компьютера (далее – НЖМД) и машинных носителях: компакт дисках (далее – CD-R/RW, DVD-R/RW в зависимости от формата), дискетах 3,5” 1,4 Mb (далее FDD), FLASH-накопителях.

Пример видов и периодов уничтожения ПД, хранимых в электронном виде представлены в Таблице №2.

Таблица № 2. Виды и периоды уничтожения ПД, хранимых в электронном виде на жестком диске компьютера

№ п/п	Информация, вид носителя	Срок хранения	Действия по окончании срока хранения
1	База данных автоматизированной информационной системы Оператора. Носитель: файлы на НЖМД сервера	До создания более актуальной копии	Повторное использование носителя для записи очередной резервной копии БД, в случае невозможности - уничтожение носителя; Удаление архивных файлов с НЖМД
2	База данных автоматизированной информационной системы «1С Предприятие-Кадры». Носитель: файлы на НЖМД сервера	До создания более актуальной копии	Повторное использование носителя для записи очередной резервной копии БД, в случае невозможности - уничтожение носителя; Удаление архивных файлов с НЖМД
3	База данных автоматизированной информационной системы «1С Бухгалтерия». Носитель: файлы на НЖМД сервера	До создания более актуальной копии	Повторное использование носителя для записи очередной резервной копии БД, в случае невозможности - уничтожение носителя; Удаление архивных файлов с НЖМД
4	Трудовая книжка, либо сведения о трудовой деятельности и трудовом стаже в электронном виде	До создания более актуальной копии	Повторное использование носителя для записи очередной резервной копии БД, в случае невозможности - уничтожение носителя; Удаление архивных файлов с НЖМД

4.2. Машинные носители информации (за исключением НЖМД), перечисленные в п.п. должны находиться в сейфе, опечатываемом печатью ответственного сотрудника (кроме формируемых или обрабатываемых в данный момент на рабочем месте).

4.3. По окончании указанных сроков хранения, машинные носители информации, подлежащие уничтожению, физически уничтожаются с целью невозможности восстановления единой целостности носителя или его сжигания.

4.4. Подлежащие уничтожению файлы, расположенные на жестком диске ПЭВМ, удаляются средствами операционной системы с последующим «очищением корзины».

4.5. В случае допустимости повторного использования носителя формата FDD, CD-RW, DVD-RW, FLASH применяется программное удаление («затирание») содержимого диска путем его формирования с последующей записью новой информации на данный носитель.

V. Порядок формирования документов об уничтожении носителей

5.1. Уничтожение носителей, содержащих ПД, осуществляет специальная комиссия, создаваемая приказом руководителя оператора. Комиссию возглавляет руководитель службы информационной безопасности оператора (или иное уполномоченное лицо). В состав комиссии должен входить сотрудник отдела автоматизации информационных систем и руководитель соответствующего подразделения оператора.

5.2. В ходе процедуры уничтожения ПД носителей необходимо присутствие членов Комиссии, осуществляющей уничтожение ПД и иной конфиденциальной информации, находящейся на технических средствах.

5.3. Комиссия составляет и подписывает Акт (2 экземпляра) об уничтожении носителей. В течение трех дней после составления акта об уничтожении направляются на утверждение руководителю оператора. После утверждения один экземпляр Акта хранится в сейфе у руководителя соответствующего подразделения оператора, второй экземпляр Акта хранится у уполномоченного оператором лица.

5.4. Факт уничтожения носителя с ПД фиксируется в «Журнале регистрации носителей информации, содержащих ПД и иную конфиденциальную информацию», где в графе «Дата и номер акта уничтожения» заносятся соответствующие данные. Данный журнал является документом конфиденциального характера и вместе с актами уничтожения хранится в сейфе.