

**УТВЕРЖДАЮ**  
Директор МБОУ СОШ №4  
*О.В. Ситник*  
Приказ № 54 от 30.03 2016г.

**ПОРЯДОК**  
**уничтожения, блокирования персональных данных**

**1. Общие положения**

Настоящий документ устанавливает порядок уничтожения информации, содержащей персональные данные, при достижении целей обработки или при наступлении иных законных оснований в Муниципальном бюджетном общеобразовательном учреждении «Средняя общеобразовательная школа № 4», в целях реализации: Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

Порядок определяет условия и способы:

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

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

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

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

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

2.3. В случае выявления неправомерных действий с персональными данными 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 персональными данными, уничтожить персональные данные.

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

2.5. Уполномоченное Оператором лицо обязано уничтожить персональные данные субъекта персональных данных в случаях:

- достижения цели обработки персональных данных оператор;
- отзыва субъектом согласия на обработку своих персональных данных.

2.6. Уничтожение персональных данных должно быть осуществлено в течение трех дней с указанных моментов. В согласии субъекта персональных данных на обработку его персональных данных могут быть установлены иные сроки уничтожения персональных данных при достижении цели обработки персональных данных. Уполномоченное Оператором лицо должно направить уведомление о факте уничтожения персональных данных субъекту персональных данных.

### 3. 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 персональные данные

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

3.2. Документы, указанные в п. 3.1., должны находиться в сейфах. Исключение составляют документы, обрабатываемые в настоящий момент на рабочем месте.

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

### 4. Работа с машинными носителями информации

4.1. Виды и периоды уничтожения персональных данных, 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“ 1.4Mb (далее – FDD), FLASH-накопителях.

Пример видов и периодов уничтожения персональных данных, хранимых в электронном виде на НЖМД, представлен в таблице 2.

Таблица 2

Виды и периоды уничтожения персональных данных, хранимых в электронном виде на жестком диске компьютера

№ п/п	Информация, вид носителя	Срок хранения	Действия по окончании срока хранения
1.	База данных автоматизированной информации	До созда-	Повторное использо-

	онной системы Оператора. Носитель: файлы на НЖМД сервера	ния более актуальной копии	вание носителя для записи очередной ре- зервной копии БД, в случае невозможности – уничтожение носите- ля; удаление архивных файлов с НЖМД
2.	База данных автоматизированной информаци- онной системы «Сотрудники предприятия». Носитель: файлы на НЖМД сервера	До созда- ния более актуальной копии	Повторное использо- вание носителя для записи очередной ре- зервной копии БД, в случае невозможности – уничтожение носите- ля; удаление архивных файлов с НЖМД
3.	База данных автоматизированной информаци- онной системы «1С Бухгалтерия». Носитель: файлы на НЖМД сервера	До созда- ния более актуальной копии	Повторное использо- вание носителя для записи очередной ре- зервной копии БД, в случае невозможности – уничтожение носите- ля; удаление архивных файлов с НЖМД

4.2. Машинные носители информации (за исключением НЖМД), перечисленные в п.п. 3.1. должны находиться в сейфе, (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 и дальнейшего использования. Это достигается путём деформирования, нарушения единой целостности носителя или его сжигания.

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

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

### **5. Порядок оформления документов об уничтожении носителей**

5.1. Уничтожение носителей, содержащих персональные данные, осуществляет специальная Комиссия, создаваемая приказом руководителя Оператора. Комиссию возглавляет ответственный за организацию обработки персональных данных. Состав комиссии не менее из двух человек.

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

5.3. Комиссия составляет и подписывает Акт (2экземпляра) об уничтожении носителей. В течение трёх дней после составления акты об уничтожении направляются на утверждение руководителю Оператора. Акты хранятся в сейфе.

5.4. Факт уничтожения носителя с персональными данными фиксируется в «Журнале регистрации носителей информации, содержащих персональные данные 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.

Муниципальное бюджетное общеобразовательное учреждение «Средняя  
общеобразовательная школа № 4»

# Журнал уничтожения носителей персональных данных

Журнал начат 01.04.2016г.  
Журнал завершён \_\_\_\_\_  
Ответственный: \_\_\_\_\_  
На 6 (шесть) листах

№ п/п	Наименование ИСПДн, в которой уничтожаются персональные данные	Ф.И.О. субъекта, перс.данные которого подлежащие уничтожению	Обоснование уничтожения	Наименование файла, и его месторасположение	Дата уничтожения	Ф.И.О. и подпись Исполнителя	Ф.И.О. и подпись ответственного за обработку персональных данных
1	2	3	4	5	6	7	8



УТВЕРЖДАЮ  
Директор МБОУ СОШ №4  
О.В. Ситник  
Приказ № 54 от 30.03 2016г.

### АКТ №

уничтожения персональных данных и иной конфиденциальной информации,  
находящейся на бумажных и технических средствах информационных систем

« \_\_\_\_\_ » \_\_\_\_\_ 20\_\_ г.  
(место уничтожения)

Комиссия в составе:

Председатель: \_\_\_\_\_  
(должность, ФИО)

Члены:

\_\_\_\_\_ (должность, ФИО)

\_\_\_\_\_ (должность, ФИО)

Составили настоящий акт в том, что « \_\_\_\_\_ » \_\_\_\_\_ 20\_\_ г. произведено уничтожение персональных данных или иной конфиденциальной информации, находящейся на

\_\_\_\_\_ (наименование АРМ по утвержденной конфигурации, ФИО ответственного Пользователя АРМ, заводской или учетный номер системного блока ПЭВМ)

№ п/п	Информация (наименование документа)	Вид носителя, учетный номер	Количество	Примечание

Перечисленные съемные носители уничтожены путем

\_\_\_\_\_ (механического уничтожения, сжигания, разрезания, демонтажа и т.п.)

Подписи членов комиссии:

\_\_\_\_\_ (должность) \_\_\_\_\_ (подпись) \_\_\_\_\_ (ФИО)

\_\_\_\_\_ (должность) \_\_\_\_\_ (подпись) \_\_\_\_\_ (ФИО)

\_\_\_\_\_ (должность) \_\_\_\_\_ (подпись) \_\_\_\_\_ (ФИО)