Муниципальное общеобразовательное бюджетное учреждение
средняя общеобразовательная школа с. Мирный
муниципального района Благоварский район Республики Башкортостан

(Наименование организации)

СОГЛАСОВАНА
с выборным органом первичной
профсоюзной организации
Протокол от 29.09.2026 №3

УТВЕРЖДЕНА
приказом директора
МОБУ СОШ с. Мирный
от 30.09.2026 №202-ОД

ИНСТРУКЦИЯ
по обращению с материальными носителями конфиденциальной информации в МОБУ СОШ с. Мирный

1. Общие положения

1.1. Настоящая инструкция определяет порядок учёта, хранения, использования, передачи и уничтожения материальных носителей, содержащих конфиденциальную информацию, в муниципальном общеобразовательном бюджетном учреждении средняя общеобразовательная школа с. Мирный муниципального района Благоварский район Республики Башкортостан (далее – Школа).

1.2. Цель инструкции – защита конфиденциальной информации от несанкционированного доступа, копирования, модификации, уничтожения и других неправомерных действий.

1.3. Инструкция разработана в соответствии с:

- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в РФ»;
- постановлением Правительства РФ от 01.11.2012 № 1119 об обеспечении защиты персональных данных в ИСПДн;
- приказом ФСТЭК России от 18.02.2013 № 21.

1.4. К конфиденциальной информации в Школе относятся:

- персональные данные обучающихся, их родителей (законных представителей);
- персональные данные работников Школы;
- сведения, составляющие служебную тайну;
- сведения об охране труда и обеспечении безопасности образовательного процесса, не подлежащие разглашению;
- иная информация, отнесённая руководством Школы к конфиденциальной.

1.5. Материальными носителями конфиденциальной информации (далее – Носители) являются:

Бумажные носители	Электронные носители
Личные дела обучающихся	USB-флеш-накопители
Журналы, тетради учёта	Внешние жёсткие диски
Медицинские карты	CD/DVD-диски
Приказы по личному составу	SD-карты, карты памяти
Заявления родителей	Ноутбуки, планшеты, смартфоны (если содержат конфиденциальную

Бумажные носители	Электронные носители
	информацию)
Отчётность по персональным данным	Системные блоки, серверы
Материалы проверок, инспекций	Бумажные распечатки, содержащие ПДн

1.6. Ответственным за организацию защиты конфиденциальной информации в Школе назначается сотрудник, ответственный за организацию обработки персональных данных (далее – Ответственный). Данное назначение оформляется приказом директора Школы.

1.7. Инструкция обязательна для исполнения всеми работниками Школы, а также иными лицами, допущенными к работе с конфиденциальной информацией (стажёры, практиканты, привлекаемые специалисты).

1.8. С инструкцией работники знакомятся под подпись при приёме на работу и при внесении изменений в инструкцию.

2. Порядок учёта носителей

2.1. Все Носители, содержащие конфиденциальную информацию, подлежат обязательному учёту.

2.2. Учёт ведёт Ответственный в **Журнале учёта материальных носителей конфиденциальной информации** (Приложение № 1).

2.3. На каждый съёмный электронный носитель (USB-флеш-накопитель, внешний жёсткий диск, CD/DVD-диск) наносится маркировка с уникальным учётным номером.

2.4. В Журнале учёта фиксируются:

- учётный номер носителя;
- тип носителя (бумажный / электронный);
- описание хранимой информации (например, «личные дела обучающихся 5 класса»);
- дата постановки на учёт;
- ФИО ответственного за хранение;
- отметки о выдаче и возврате (дата, подпись получившего и вернувшего);
- отметка об уничтожении (дата, номер акта).

2.5. Бумажные носители учитываются как единые комплексы (например, «Личные дела обучающихся 1 класса – 25 шт.») либо индивидуально – по решению Ответственного.

2.6. Носители, не состоящие на учёте в Журнале, к использованию в Школе **запрещены**.

2.7. При выявлении неучтённого носителя сотрудник обязан сообщить об этом Ответственному не позднее конца рабочего дня.

3. Порядок хранения носителей

3.1. Хранение Носителей должно исключать доступ к ним лиц, не допущенных к конфиденциальной информации.

3.2. Бумажные носители хранятся:

- в запираемых шкафах, сейфах или специально отведённых помещениях;
- ключи от шкафов и сейфов хранятся у лица, ответственного за хранение; дубликаты ключей – у Ответственного или директора Школы в опечатанном конверте;
- по окончании рабочего дня шкафы и сейфы запираются, помещения опечатываются.

3.3. Электронные носители хранятся:

- в опечатанных или запираемых ящиках (сейфах) в помещении, где расположены технические средства;
- в защищённом от пыли, влаги, прямых солнечных лучей и электромагнитных полей

месте;

- съёмные носители – в отдельной маркированной таре (коробка, конверт) с указанием учётного номера.

3.4. **Запрещается** хранить Носители совместно с носителями открытой информации (учебные материалы, объявления, методические разработки, не содержащие ПДн).

3.5. Запрещается оставлять Носители на рабочих столах, в незапертых ящиках столов, на подоконниках и в других местах, доступных посторонним.

3.6. Хранение Носителей вне помещений Школы (на дому, в личном транспорте) **не допускается**, за исключением случаев, прямо предусмотренных разделом 4 настоящей инструкции.

4. Порядок использования и передачи носителей

4.1. Работа с Носителями разрешается **только** в помещениях Школы и **только** в рамках исполнения должностных обязанностей.

4.2. Перед использованием съёмного электронного носителя сотрудник обязан убедиться, что носитель:

- состоит на учёте (имеет маркировку);
- не имеет видимых повреждений;
- проверен антивирусными средствами (для электронных носителей — при наличии технической возможности).

4.3. При работе с электронными носителями:

- подключение съёмных носителей к рабочим компьютерам Школы разрешается только после проверки на вредоносное ПО штатными антивирусными средствами;
- запись конфиденциальной информации на личные (неучтённые) носители **запрещена**;
- копирование конфиденциальной информации на неучтённые носители других работников **запрещено**.

4.4. Передача Носителей между работниками Школы оформляется:

- записью в Журнале учёта (для съёмных электронных носителей и учтённых бумажных комплексов);
- под подпись в графе «выдал» и «получил».

4.5. Вынос Носителей за пределы Школы:

- **запрещён** по умолчанию;
- допускается **только** с письменного разрешения директора Школы (или лица, исполняющего обязанности);
- основание для выноса – служебная необходимость (участие в проверке, выездное мероприятие, передача в вышестоящую организацию);
- при выносе Носитель помещается в упаковку, исключающую случайное открытие и позволяющую выявить попытку вскрытия (опечатанный конверт, заклеенный пакет с печатью).

4.6. Передача Носителей сторонним организациям (органы управления образованием, Рособрнадзор, прокуратура, иные ведомства) осуществляется:

- на основании официального запроса;
- по акту приёма-передачи (Приложение № 2);
- с фиксацией факта передачи в Журнале учёта.

4.7. Передача Носителей по электронной почте, через мессенджеры или иные сетевые каналы связи **запрещена**, за исключением использования сертифицированных защищённых каналов, если такие предусмотрены технической политикой Школы.

5. Ограничения и запреты

5.1. Работникам Школы **запрещается**:

- использовать Носители в личных целях;

- передавать Носители лицам, не допущенным к работе с конфиденциальной информацией (в том числе другим работникам Школы, не имеющим соответствующих полномочий);
- самостоятельно копировать, размножать, тиражировать конфиденциальную информацию без разрешения Ответственного или директора;
- выносить Носители из помещений Школы без разрешения (раздел 4);
- сообщать пароли, коды доступа к электронным Носителям и оборудованию лицам, не имеющим к ним доступа;
- фотографировать, сканировать, копировать экраны с конфиденциальной информацией на личные устройства;
- оставлять включённый компьютер без блокировки экрана при отсутствии на рабочем месте;
- подключать личные мобильные устройства к компьютерам Школы для зарядки или передачи данных.

5.2. Не допускается обсуждение содержания Носителей в присутствии лиц, не допущенных к данной информации (в том числе в коридорах, столовой, на совещаниях открытого формата).

6. Действия в нештатных ситуациях

6.1. При выявлении любого из следующих событий работник обязан **немедленно** (в день выявления) сообщить Ответственному и директору Школы:
- утрата, хищение Носителя;
- повреждение Носителя (механическое, термическое, затопление);
- подозрение на несанкционированный доступ (следы вскрытия упаковки, неавторизованное подключение, появление незнакомых файлов);
- разглашение конфиденциальной информации (устное, письменное, через сеть);
- заражение электронного носителя вредоносным ПО.

6.2. По факту утраты или повреждения Ответственный:
- составляет служебную записку на имя директора;
- проводит внутреннее расследование (при необходимости);
- вносит соответствующую отметку в Журнал учёта;
- принимает меры по предотвращению дальнейших рисков (блокировка учётных записей, смена паролей, уведомление компетентных органов).

6.3. При факте разглашения персональных данных Школа руководствуется требованиями ст. 21 Федерального закона № 152-ФЗ: оценивает угрозу, информирует субъекта персональных данных (при необходимости), уведомляет Роскомнадзор в установленный срок.

6.4. До прибытия Ответственного работник, выявивший нештатную ситуацию, обязан:
- обеспечить сохранность места происшествия (не трогать предметы, не отключать оборудование без необходимости);
- прекратить работу с Носителем, вызвавшим подозрение.

7. Порядок уничтожения носителей

7.1. Уничтожению подлежат Носители, которые:
- пришли в негодность (физический износ, повреждение);
- выработали установленный срок эксплуатации;
- более не используются (информация потеряла актуальность, истёк срок хранения, предусмотренный номенклатурой дел).

7.2. Решение об уничтожении принимает директор Школы на основании служебной записки Ответственного.

7.3. Уничтожение должно **полностью исключать** возможность восстановления

информации.

7.4. Способы уничтожения:

Тип носителя	Способ уничтожения
Бумажные документы	Сжигание или измельчение на шредере (фрагменты не более 3×3 мм)
USB-флеш-накопители	Физическое разрушение (разрушение чипа), затем утилизация
CD/DVD-диски	Физическое разрушение (измельчение, излом)
Внешние жёсткие диски	Многократная перезапись спецпрограммой, затем физическое разрушение
Системные блоки, серверы	Многократная перезапись или размагничивание, затем утилизация в установленном порядке

7.5. Уничтожение проводится комиссией в составе не менее трёх человек, назначаемой приказом директора Школы.

7.6. По результатам уничтожения составляется **Акт об уничтожении материальных носителей конфиденциальной информации** (Приложение № 3), который подписывается всеми членами комиссии и утверждается директором.

7.7. После уничтожения в Журнале учёта делается отметка с указанием номера Акта и даты уничтожения.

8. Ответственность

8.1. Работники Школы, нарушившие требования настоящей инструкции, несут ответственность в соответствии с действующим законодательством:

- дисциплинарную (замечание, выговор, увольнение);
- гражданско-правовую (возмещение ущерба);
- административную (ст. 13.11 КоАП РФ – за нарушение законодательства о персональных данных);
- уголовную (ст. 137, 138, 272 УК РФ – при наличии состава преступления).

8.2. Контроль за соблюдением инструкции осуществляет Ответственный и директор Школы.

8.3. Проверки соблюдения требований проводятся не реже одного раза в полугодие. Результаты проверки оформляются справкой (актом), представляемой директору.

9. Заключительные положения

9.1. Инструкция вступает в силу с момента её утверждения приказом директора Школы.

9.2. Изменения и дополнения в инструкцию вносятся приказом директора по представлению Ответственного.

9.3. Инструкция пересматривается не реже одного раза в три года, а также при изменении законодательства или существенных изменениях в организации обработки информации в Школе.

Приложение № 1 к Инструкция
по обращению с материальными носителями
конфиденциальной информации
в МОБУ СОШ с. Мирный

Журнал учёта материальных носителей конфиденциальной информации

№ п/п	Учётный номер	Тип носителя	Описание информации	Дата постановки на учёт	ФИО ответственного	Выдача (дата, ФИО, подпись)	Возврат (дата, ФИО, подпись)	Отметка об уничтожении (№ акта, дата)
1	МН-001	USB-флеш 16 ГБ	ПДн обучающихся 5-А	01.09.2026	Иванова А.А.			
2	МН-002	Бумажный	Личные дела работников	01.09.2026	Петрова О.С.			

Приложение № 2 к Инструкция
по обращению с материальными носителями
конфиденциальной информации
в МОБУ СОШ с. Мирный

УТВЕРЖДАЮ
Директор _____
(наименование Школы)
_____ /_____
(подпись) (Ф.И.О.)
«___» _____ 20___ г.

АКТ
приёма-передачи материальных носителей
конфиденциальной информации

Дата: «___» _____ 20___ г.

Школа (передающая сторона) в лице _____
(должность, ФИО)
передает, а _____
(принимающая сторона)
в лице _____
(должность, ФИО)
Принимает следующие материальные носители:

№ п/п	**Учётный номер**	**Тип носителя**	**Описание информации**
1			
2			

Всего передано: _____ шт.

Информация о носителях достоверна и соответствует записям
в Журнале учёта.

Передал: _____ /_____/
М.П.

Принял: _____ /_____/
М.П.

Приложение № 3 к Инструкция
по обращению с материальными носителями
конфиденциальной информации
в МОБУ СОШ с. Мирный

УТВЕРЖДАЮ
Директор _____
(наименование Школы)
_____ /_____
(подпись) (Ф.И.О.)
«___» _____ 20___ г.

АКТ
об уничтожении материальных носителей
конфиденциальной информации

Дата: «___» _____ 20___ г.

Составлен комиссией в составе:
Председатель: _____ /_____/
Члены комиссии: _____ /_____/
_____ /_____/

На основании приказа № ___ от «__» _____ 20__ г. провела уничтожение следующих материальных носителей:

№ п/п	Учётный номер	Тип носителя	Описание информации	Способ уничтожения
1				
2				

Всего уничтожено: ___ шт.

Уничтожение проведено способом, исключающим восстановление информации.

Члены комиссии:

Председатель: _____ /_____/
Члены: _____ /_____/
_____ /_____/