ПРИНЯТО
педагогическим советом
МКОУ «Каракюринская СОШ»
Протокол № 05 от 27.05.2020г.

УТВЕРЖДЕНО
директор школы
Гаджибеков Э.А.
«_27_» ___05__ 2020___ г.

Порядок доступа работников МКОУ «Каракюринская СОШ имени Г. М. Махмудова» в помещения, в которых ведется обработка персональных данны

1.1. Настоящий Порядок определяет процедуру доступа работников МКОУ «Каракюринская СОШ» (далее - Учреждение) в помещения, в которых ведется обработка персональных данных и разработан в соответствии с постановлением Правительства Российской Федерации от 21 марта 2012 года
№ 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных
Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных».
1.2. Целью настоящего Порядка является обеспечение исключения неправомерного или случайного доступа к материальным носителям персональных данных и техническим средствам их обработки, а также иных неправомерных действий в отношении персональных данных.

2. Порядок доступа в помещения, в которых ведется обработка персональных данных
2.1. Доступ работников МКОУ «Каракюринская СОШ», в помещения, в которых ведется обработка персональных данных, осуществляется согласно перечню должностей работников МКОУ «Каракюринская СОШ», допущенных к обработке персональных данных, утвержденным приказом директора.
2.2. Допуск в помещения, в которых ведется обработка персональных данных, иных лиц, осуществляется работниками, указанными в Разрешительной системе доступа работников МКОУ «Каракюринская СОШ» в помещения, в которых ведется обработка персональных данных. Пребывание посторонних лиц в кабинетах, в которых ведется обработка персональных данных, допускается только в присутствии работников, указанных в Разрешительной системе доступа работников МКОУ «Каракюринская СОШ», допущенных в помещения, в которых ведется обработка персональных данных.
2.3. Работники контролирующих органов допускаются в помещение (отделения), в котором ведется обработка персональных данных, при наличии соответствующего предписания на проведение контрольных мероприятий с разрешения директора МКОУ «Каракюринская СОШ», (лица , его замещающего) в его присутствии или лица, его замещающего.

2.4. Работники сторонних организаций, прибывшие в помещение, в котором ведется обработка персональных данных, для выполнения работ, оказания услуг в соответствии с заключенными государственными контрактами (договорами) допускаются в помещение с разрешения директора МКОУ «Каракюринская СОШ» (лица его замещающего) на основании информации, полученной от ответственного за организацию и выполнение работ по государственному контракту (договору).

2.5. При проведении таких работ работники отделения обязаны принять меры по исключению ознакомления работников сторонних организаций с персональными данными.

3. Порядок вскрытия и сдачи под охрану помещений, в которых ведется обработка персональных данных.

3.1. Помещения, в которых ведется обработка персональных данных, по окончании рабочего дня должны закрываться на ключ.

Ключи от замков передаются и находятся на ответственном хранении у сотрудников отделений, работающих в служебных помещениях, а также у сотрудника, уполномоченного хранить резервные ключи от замков всех помещений.

3.2. Вскрытие и закрытие помещения осуществляют сотрудники отделения, допущенные в данное помещение.

3.3. При завершении рабочего дня сотрудники отделений обязаны выполнить следующие мероприятия:

- убрать документы с персональными данными в шкафы, сейфы или запирающиеся на ключ шкафы;
- выключить установленным порядком вычислительную технику и оргтехнику;
- закрыть окна;
- выключить электроприборы;
- выключить свет;
- закрыть входную дверь на замок;
- ключ от входной двери в помещение сотрудник отделения сохраняет у себя;

3.4. Сотрудники, вскрывающие помещение, в котором ведется обработка персональных ,данных, обязаны выполнить следующие мероприятия:

- проверить целостность входной двери помещения;
- вскрыть помещение;
- проверить целостность сейфа (шкафа, тумбочек), наличие и целостность компьютерной и оргтехники;
- при обнаружении нарушения целостности двери, сейфа, шкафа , тумбочек, отсутствии или нарушении целостности

вычислительной техники, других нарушениях сотрудник, вскрывающий помещение, в котором ведется обработка персональных данных, обязан прекратить вскрытие помещения, доложить о выявленных нарушениях своему непосредственному руководителю .

4. Запрещается

4.1. Запрещается оставлять помещения, в которых ведется обработка персональных данных, без присмотра работников, имеющих допуск в помещения, где ведется обработка персональных данных.

4.2. Запрещается оставлять без присмотра находящихся в помещении, в которых ведется обработка персональных данных, посторонних лиц, а также, работников, не имеющих допуск в помещения, в которых ведется обработка персональных данных.

5. Внутренний контроль

5.1. Внутренний контроль за соблюдением порядка доступа в помещения, в которых ведется обработка персональных данных, осуществляется лицом, ответственным за обработку персональных данных.

6. Ответственность

6.1. Работники, нарушившие нормы настоящего Порядка, несут ответственность в соответствии с действующим законодательством.

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).	установлены е для данных документов сроки хранения	Уничтожение
3.	Другие документы 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, опечатываемых 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 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" 1.4МЬ (далее - FDD), FLASH-накопителях.

Пример видов и периодов уничтожения персональных данных, хранимых в электронном виде 1-1а 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	Действиs1 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. Носитель: файлы на НЖМД сервера	До создания более актуальной **копии**	Повторное использование носите ля для записи очередной резервной копии БД, в случае невозможности - уничтожение носителя ; удаление архивных файлов с НЖМД
3.	База данных автоматизированной информационной системы «IC Бухгалтерия». Носитель: файлы на НЖМД сервера .	До создания более актуальной **копиии**	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. 3.1. 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 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 носит ель.

5. Порядок оформления документов об уничтожении носителей

5. 1 . Уничтожение носителей, содержащих персональные данные, 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 автоматизированных информационных систем и руководитель соответствующего подразделения Оператора.

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

5.3. Комиссия составляет и подписывает Акт (2 экземпляра) об уничтожении носителей. В течение трёх дней после составления акты 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 руководителя службы информационной безопасности Оператора.

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.

ПРИНЯТО
педагогическим советом
МКОУ «Каракюринская СОШ»
Протокол от _____2019г.№1

УТВЕРЖДЕНО
директор школы
Гаджибеков Э.А. _____
«___» _____ 20___ г.

ПОРЯДОК
уничтожения, блокирования персональных данных в МКОУ «Каракюринская СОШ»

1. Общие положения

Настоящий 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