Комитет по образованию Администрации г.Улан-Удэ
Муниципальное автономное общеобразовательное учреждение
«Средняя общеобразовательная школа № 5 г. Улан-Удэ»

ПРИКАЗ

от «31» августа 2021 г. № 311

О назначении ответственным лиц
за обработку персональных данных
МАОУ «СОШ №5»
в 2021-2022 учебном году

В соответствии с Федеральным законом от 27.07.2006 г. N. 152-ФЗ «О персональных данных» (с изм. от 2.07.2021г.), Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» в целях обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных

ПРИКАЗЫВАЮ:

1. Назначить ответственными по обработке персональных данных следующих сотрудников МАОУ «СОШ №5»:

№	Лица, допущенные к обработке персональных данных	Группы обрабатываемых в МАОУ «СОШ №5» персональных данных
1	Директор школы Зайцева Е.М.	Все персональные данные по сотрудникам и обучающимся школы
2	Системный администратор Машанов А.Н.	Все персональные данные по сотрудникам иобучающимся школы
3	Социальные педагоги школы: Сафонова О.И. Сосорова С.Ц.	Данные о социальных и жилищных условиях, о материальном положении обучающихся
4	Заместители директора по учебно-воспитательной работе: Базилевская О.П. Санжиева Ц.С. Шкурлова М.В.	Данные о преподаваемых предметах, о дополнительной педагогической нагрузке, о научно-методической работе, сведения об образовании, стаже, аттестации и повышении квалификации, о наградах и достижениях

5	Специалист по кадрам/секретарь Ефимова Н.С.	Все персональные данные по сотрудникам, информация о фактическом месте проживания работников и контактные телефоны
6	Специалист по безопасности: Мальцева О.С. Специалист по ОТ: Петрова В.В.	Информация о фактическом месте проживания работников и обучающихся и контактные телефоны
7	Библиотекарь: Попова Ж.И.	Персональные данные обучающихся школы

2. Ознакомить сотрудников, указанных в п.1 настоящего приказа с инструкцией пользователя при обработке персональных данных (Приложение 1 к приказу).

3. Утвердить перечень помещений в МАОУ «СОШ №5» для обработки персональных данных: п.Сосновый Бор, ул.Бонивура, 40 (каб. директора, приемная, библиотека, замдиректоров)

4. Утвердить положение о режиме обеспечения безопасности помещений, в которых размещена информационная система, препятствующем возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения (Приложение 2 к приказу).

5. Назначить Машанова А.Н., системного администратора, ответственным за организацию обработки персональных данных в МАОУ «СОШ №5».

6. Возложить на Машанова А.Н. следующие обязанности:

- осуществление внутреннего контроля за соблюдением МАОУ «СОШ №5» и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- доведение до сведения работников МАОУ «СОШ №5» положений законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- осуществление контроля за приемом и обработкой обращений и запросов субъектов персональных данных или их представителей;
- составление уведомлений уполномоченного органа по защите прав субъектов персональных данных об обработке персональных данных, об изменениях в реквизитах оператора персональных данных.

7. Контроль за выполнением настоящего приказа оставляю за собой.

Директор МАОУ «СОШ №5» /Зайцева Е.М.

Приложение1

Инструкция пользователя при обработке персональных данных

Настоящей инструкцией определяется порядок защиты персональных данных обрабатываемых средствами вычислительной техники в соответствии с Федеральным законом от 27 июня 2006 года № 152-ФЗ «О персональных данных» (с изм. от 2.07.2021г.), Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

1. Персональные данные, содержащиеся в информационных ресурсах в ГБОУ Школа № 1504, относятся к сведениям конфиденциального характера, имеют ограниченный доступ и разглашению не подлежат за исключением персональных данных, на которые в соответствии с федеральными законами не распространяются требования о соблюдении конфиденциальности.

2. Для целей настоящей инструкции используются следующие основные понятия:

- персональные данные — любая информация, относящаяся к определенному или определяемому на основании такой информации гражданина, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;
- обработка персональных данных — сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение персональных данных.
- использование персональных данных — действия (операции) с персональными данными, совершаемые сотрудником имеющего доступ к персональным данным администрации в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении граждан либо иным образом затрагивающих их права и свободы или права и свободы других лиц;
- уничтожение персональных данных — действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;
- общедоступные персональные данные — персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия лица или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.
- информация — сведения (сообщения, данные) независимо от формы их представления.

3. В обязанности сотрудника, имеющего доступ к персональным данным, обрабатываемым средствами вычислительной техники, осуществляющего получение, обработку, хранение, передачу и любое другое использование персональных данных, содержащихся в информационных ресурсах входит:

- обеспечение сохранности информационных ресурсов;
- обеспечение конфиденциальности сведений, содержащихся в информационных ресурсах, в соответствии с федеральными законами, иными нормативными актами Российской Федерации;

4. Передача третьей стороне персональных данных, содержащихся в информационных ресурсах, не допускается, за исключением случаев, установленных федеральными законами.

5. Хранение информационных ресурсов должно осуществляться в условиях, исключающих возможность доступа к ним лиц, не уполномоченных на получение, обработку, хранение, передачу и любое другое использование персональных данных, содержащихся в информационных ресурсах.

6. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

7. Сотрудник, имеющий доступ к персональным данным, содержащимся в информационных ресурсах, может привлекаться в соответствии с законодательством Российской Федерации к дисциплинарной и иной ответственности за разглашение персональных данных.

Лист ознакомления пользователей
с инструкцией по обработке персональных данных

№ о/о	Фамилия, имя, отчество	Дата ознакомления с инструкцией	Подпись
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
t 0.			
1 i.			
12.			
13.			
14.			
15.			
16.			
17.			
18.			
19.			
20.			
21.			
22.			
23.			

Приложение 2

ПОЛОЖЕНИЕ

о режиме обеспечения безопасности помещений, в которых размещена информационная система, препятствующем возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа вэти помещения

1 Общие положения

1.1. Настоящий документ определяет порядок обеспечения безопасности помещений МАОУ «СОШ №5» (далее — образовательная организация), в которых размещены компоненты информационных систем персональных данных. препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.

1.2. Настоящий документ не определяет задачи пропускного и внутри объектового режима, поскольку пропускной и внутриобъектовый режим в образовательной организации установлен соответствующим приказом директора образовательной организации.

1.3. Пропускной и внутриобъектовый режим обеспечивает исключение несанкционированного прохода обучающихся, законных представителей обучающихся, работников и посетителей на территорию и в здания образовательной организации, ввоза (вывоза), вноса (выноса) ими материальных ценностей.

1.4. Все работники, принимаемые в структурные подразделения образовательной организации, ознакамливаются под подпись с настоящим положением.

2 Размещение компонентов информационных систем

2.1. Все компоненты информационных систем — автоматизированные рабочие места, серверы, сетевое оборудование — должны находиться в служебных помещениях на максимально возможном отдалении от границ контролируемой зоны.

2.2. Силовые и телекоммуникационные кабели должны быть защищены от помех или повреждений с помощью размещения в защищенных боксах, изолированных каналах.

2.3. Мониторы и другие средства отображения информации должны располагаться таким образом, чтобы исключить несанкционированный просмотр третьими лицами.

2.4. Оконные проемы помещений, в которых находятся компоненты информационных систем, должны быть закрыты жалюзи.

2.5. Автоматизированные рабочие места, сетевое оборудование, серверы и специализированные шкафы для оборудования должны быть опечатаны.

2.6. Должно блокироваться несанкционированное подключение устройств и съемных носителей информации к компонентам информационных систем путем отключения или блокирования разъемов на серверном оборудовании и программного блокирования на автоматизированных рабочих местах.

3 Организация доступа в помещения

3.1. В отношении каждого служебного помещения образовательной организации должен быть определен перечень лиц (должностей), имеющих к ним доступ.

3.2. Лица, не имеющие доступа к помещениям, не должны иметь возможности самостоятельного доступа без сопровождения в помещения, в

которых размещаются компоненты информационных систем, а также носители информации.

3.3. Работник, сопровождающий посетителей, должен постоянно контролировать действия посетителей.

3.4. Служебное помещение в отсутствие работника, имеющего к нему доступ, должно быть закрыто на механический замок.

3.5. Служебные помещения открываются и закрываются самими работниками.

Должна быть реализована процедура контроля и учета ключей:

- ключи и журнал учета ключей должны храниться у на посту охраны;
- ключи должны выдаваться в соответствии со списками лиц, имеющих доступ в защищаемые помещения, и под личную подпись
- должен фиксироваться работник, которому были выданы ключи, дата и время выдачи, а также отметки о сдаче ключей.

3.6. Уборка или иные работы в помещениях, в которых размещаются компоненты информационных систем, должны производиться в присутствии ответственного работника с соблюдением мер, исключающих доступ посторонних лиц к защищаемым ресурсам.

Приложение 3

Перечень лиц, ответственным за реализацию мер по обеспечению сохранности персональных данных без использования средств автоматизации и исключениюнесанкционированного к ним доступа

N.°	Фамилия, Имя, Отчество	**Должность**
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		
18.		
19.		
20.		
21.		
22.		
23.		