Муниципальное бюджетное общеобразовательное учреждение
«Основная общеобразовательная школа №280»
п. Оленья Губа имени Героя Российской Федерации
Дениса Александровича Опарина

ПРИКАЗ

29.08.2022 г. **№ 263**

Об утверждении пакета документов по обработке персональных данных

Руководствуясь требованиями Федеральных законов от 27 июля 2006г. № 152-ФЗ «О персональных данных», от 27 июля 2006г., № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

ПРИКАЗЫВАЮ:

1. Утвердить:

1.1. Положение по обработке персональных данных в МАОУ «ООШ № 280» (Приложение №1);
1.2. Форму согласия родителя (законного представителя) обучающегося на обработку персональных данных (Приложение № 2);
1.3. Дополнение в договор оказания образовательных услуг (Приложение № 3);
1.4. Перечень сведений конфиденциального характера в МАОУ «ООШ № 280» (Приложение № 4);
1.5. Положение об ответственности работников, допущенных к обработке персональных данных и иной конфиденциальной информации (Приложение № 5);
1.6. Форму Соглашения (обязательства) о неразглашении персональных данных работников и форму Соглашения (обязательства) о неразглашении персональных данных учащихся, воспитанников, родителей (законных представителей) (Приложение № 6);
1.7. Положение об обеспечение безопасности автоматизированных информационных систем МАОУ «ООШ № 280» (Приложение № 7);
1.8. Положение о парольной защите при обработке персональных данных и иной конфиденциальной информации (Приложение № 8);
1.9. Инструкция о применении средств антивирусной защиты информации (Приложение № 9);
1.10. Регламент использования программного обеспечения (Приложение № 10);
1.11. Регламент использования электронной почты в образовательной организации (Приложение № 11);
1.12. Памятка по работе с корпоративной электронной почтой МАОУ «ООШ № 280» (Приложение № 12);
1.13. Регламент доступа и использования ресурсов сети интернет в МАОУ «ООШ № 280» (Приложение № 13);

1.14. Порядок учета и использования машинных носителей информации, содержащих персональные данные и иную конфиденциальную информацию (Приложение № 14);
1.15. Требования к оборудованию помещений и размещению технических средств, используемых для обработки персональных данных (Приложение № 15);
1.16. Порядок уничтожения, блокирования персональных данных (Приложение № 16);
1.17. Форму акта уничтожения персональных данных и иной конфиденциальной информации, находящейся на технических средствах информационных систем (приложение № 17);
1.18. Форму акта выявления нарушений в сфере защиты персональных данных и иной конфиденциальной информации (Приложение № 18);
1.19. Форму журнала регистрации выявления нарушений в сфере защиты персональных данных и иной конфиденциальной информации (Приложение № 19);
1.20. Положение о службе информационной безопасности МАОУ «ООШ № 280» (Приложение № 20);
1.21. Форму журнала регистрации используемого программного обеспечения (ПО) (Приложение № 21);
1.22. Форму журнала учета носителей, содержащих персональные данные и иную конфиденциальную информацию (Приложение № 22);

2. Заместителю директора по учебной работе (УР), старшему воспитателю при оформлении приема обучающихся:
2.1. Обеспечить получение Согласий по установленной форме от всех обучающихся и/или их законных представителей.
2.2. Довести данный пакет документов по обработке персональных данных до сведения заместителя директора по воспитательной работе.
3. Секретарю учебной части обеспечивать получение Согласий по установленной форме от всех работников образовательной организации. Для вновь принимаемых обучающихся и работников получение Согласий проводить в соответствии с утвержденным Положением.
3.1. При оформлении трудовых договоров, дополнительных соглашений к трудовым договорам вносить пункт «Обработка персональных данных».
3.2. Ознакомить сотрудников, занимающих должности, перечисленные в п. 5 настоящего приказа с пакетом документов по обработке персональных данных под роспись.
4. Заместителю директора по воспитательной работе (ВР) при оказании образовательных услуг на договорной основе включать в договор раздел «Обработка персональных данных».
5. Допустить до обработки персональных данных в части их касающихся работников следующих должностей:

№ п/п	Должность
1.	директор
2.	заместитель директора по УР
3.	заместитель директора по ВР
4.	главный бухгалтер

5.	ведущий бухгалтер
6.	ведущий экономист
7.	бухгалтер
8.	учитель начальных классов, классный руководитель
9.	учитель, классный руководитель
10.	преподаватель-организатор ОБЖ, классный руководитель, инженер
11.	педагог-психолог
12.	учитель-логопед
13	социальный педагог, классный руководитель
14.	библиотекарь, секретарь учебной части, делопроизводитель
15.	учитель
16.	старший воспитатель
17.	инструктор по физической культуре
18.	музыкальный руководитель
19.	воспитатель
20.	советник директора по воспитанию

6. Назначить руководителем службы информационной безопасности заместителя директора по воспитательной работе Крапива Н.В.
7. Руководителю службы информационной безопасности Крапива Н.В.:

7.1. Организовать деятельность службы информационной безопасности в соответствии с утвержденным Положением.

7.2. Разработать и представить на утверждение в срок до 09.09.2022г. план работы по обеспечению информационной безопасности организации на 2022/2023 учебный год.

8. Исполнение обязанностей администратора, отвечающего за обеспечение образовательной организации программным обеспечением и информационными ресурсами (далее-Администратор), возложить на Шарова А.В., инженера.
9. Администратору Шарову А.В. довести Регламент до 01.09.2022г. до сведения заместителей директора, пользователей персональных компьютеров под роспись в листе ознакомления.

9.1. Обеспечить ведение учета используемого программного обеспечение в Журнале.

10. Приказ вступает в силу с момента его подписания.
11. Считать утратившим силу приказ № 128 от 30.05.2017г. «Об утверждении пакета документов об обработке персональных данных».
12. Контроль за исполнением настоящего приказа оставляю за собой.

Директор МАОУ «ООШ № 280» **Е.П. Пятницкая**

Приложение № 1
к приказу от 29.08.2022 № 263

Положение
по обработке персональных данных в МАОУ «ООШ № 280»

1. Общие положения

1.1. Согласно статьи 23 Конституции Российской Федерации каждый имеет право на неприкосновенность частной жизни, личную, семейную тайну, защиту своей чести и доброго имени, реализация которого обеспечивается положением статьи 24 Конституции, устанавливающим, что сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускается. Отношения, связанные с обработкой персональных данных, осуществляемой юридическими лицами с использованием средств автоматизации или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, регулируются Федеральным законом от 27 июля 2006 г. N 152-ФЗ "О персональных данных".

Настоящее Положение разработано в целях выполнения указанных выше норм Конституции РФ, в соответствии с требованиями законодательства Российской Федерации и иных нормативных правовых актов в сфере образования и обработки персональных данных.

1.2. Настоящее Положение определяет порядок работы (получения, обработки, использования, передачи, хранения и т.д.) МАОУ «ООШ № 280» (далее Оператор) с персональными данными обучающихся, работников и гарантии конфиденциальности сведений об обучающемся, работнике, предоставленных ими в образовательной организации; права обучающегося, работника при обработке их персональных данных; ответственность лиц за невыполнение требований норм, регулирующих обработку персональных данных.

2. Понятие и состав персональных данных

2.1. Персональные данные - любая информация, относящаяся прямо или косвенно к обучающемуся, работнику (субъекту персональных данных).

2.2. К персональным данным относятся следующие сведения:

- фамилия, имя, отчество;
- пол;
- дата рождения;
- место рождения;
- гражданство;
- адрес места жительства и домашний телефон;
- номер мобильного телефона;
- сведения о состоянии здоровья, предоставляемые в установленном порядке, т.е. при поступлении в образовательное учреждение, а также при прохождении периодических медицинских осмотров или в иных случаях;
- сведения о полученном ранее образовании;
- сведения о месте жительства, месте работы и номера служебных и домашних телефонов законных представителей обучающегося;
- иные сведения об обучающемся или работнике.

Все персональные данные, касающиеся состояния здоровья обучающегося, работника

относятся к специальным категориям персональных данных и обрабатываются в соответствии с установленным законодательством и иными нормативными правовыми актами требованиями.

3. Сбор, цели обработки и защита персональных данных

3.1. Обработка персональных данных осуществляется:

3.1.1. После получения письменного согласия обучающегося (или его законных представителей), работника, составленного по утверждённой Оператором форме, соответствующей требованиям федерального закона, за исключением случаев, предусмотренных частью 2 статьи 6 Федерального закона № 152-ФЗ от 27 июля 2006 г. «О персональных данных»;

3.1.2. После заключения с обучающимся (с законными представителями), договора об оказании образовательных услуг (если обучение осуществляется на договорной основе), в котором определены доверие и обязанность по обработке персональных данных. В этом случае в соответствии с п. 2) части 2 статьи 6 ФЗ «О персональных данных» в целях исполнения договора об оказании образовательных услуг, одной из сторон которого является субъект персональных данных, т.е. обучающийся, и получения его согласия на обработку персональных данных не требуется;

3.1.3. После направления уведомления об обработке персональных данных в орган государственного надзора в сфере связи, информационных технологий и массовых коммуникаций территории, за исключением случаев, предусмотренных частью 2 статьи 22 Федерального закона «О персональных данных»;

3.1.4. После принятия Оператором необходимых мер по защите персональных данных.

3.2. Все персональные данные обучающегося, работника следует получать лично у обучающегося (при условии, что на момент предоставления таких данных обучающийся является дееспособным) или его законного представителя, а также у работника.

3.3. Оператор сообщает обучающемуся или его законному представителю, работнику о целях обработки персональных данных, предполагаемых источниках и способах получения персональных данных и последствиях отказа обучающегося или его законного представителя, работника дать письменное согласие на их получение.

3.4. Оператор осуществляет обработку персональных данных только после получения письменного согласия обучающегося (или его законного представителя), работника на обработку его персональных данных за исключением случаев, предусмотренных действующим законодательством.

3.5. При обращении в образовательную организацию гражданин (или его законный представитель) предоставляет Оператору персональные данные о себе в документированной форме в соответствии с установленными нормативными правовыми актами требованиями.

3.6. Оператор с согласия обучающегося (или его законного представителя), работника может запрашивать и получать персональные данные обучающегося, работника используя информационные системы персональных данных с применением средств автоматизации.

3.7. Обработка Оператором персональных данных обучающегося осуществляется исключительно в целях оказания обучающемуся качественных образовательных услуг в необходимом объёме, соблюдения требований действующего законодательства, иных нормативных правовых актов, обеспечения контроля объёмов и качества обучения.

3.8. Оператор при определении объёма и содержания обрабатываемых персональных данных руководствуется Конституцией Российской Федерации, иными нормативными правовыми актами в сфере образования и обработки персональных данных.

3.9. Защита персональных данных от неправомерного их использования или утраты обеспечивается Оператором за счет собственных средств в порядке, установленном законодательством, и принятыми Оператором в соответствии с ним локальными нормативными актами.

4. Порядок использования, хранения, передачи персональных данных

4.1. Персональные данные обучающегося, работника предоставляются Оператору после получения соответствующего согласия обучающегося (или его законного представителя), работника на обработку его персональных данных. Персональные данные у Оператора содержаться в информационных системах персональных данных, представляющих собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств. В информационных системах персональные данные могут быть размещены на материальных, в том числе бумажных носителях.

4.2. Доступ к обработке персональных данных (как с использованием средств автоматизации, так и без использования средств автоматизации) обеспечивается в установленном Оператором порядке.

4.3. Конкретные обязанности по работе с информационными системами персональных данных и материальными носителями информации, в том числе с документами, содержащими персональные данные возлагаются на сотрудников Оператора и закрепляются в должностных инструкциях.

4.4. Работа с информационными системами персональных данных, материальными носителями, в том числе с документацией, содержащими персональные данные осуществляется в специально отведённых для этого помещениях: учебный отдел, серверная и т.д.

4.5. Требования к месту обработки персональных данных, в том числе к серверной, обеспечивающие их защищённость устанавливаются Оператором.

4.6. Перечень лиц, имеющих право доступа к персональным данным обучающихся, работников и обработке их персональных данных, определяется приказом руководителя Оператора.

4.7. С лицами, допущенными к обработке персональных данных обучающихся, работников заключается Соглашение о неразглашении.

4.8. Лица, допущенные в установленном порядке к обработке персональных данных, имеют право обрабатывать только те персональные данные обучающихся, работников, которые необходимы для выполнения конкретных функций.

4.9. Оператор при создании и эксплуатации информационных систем персональных данных с использованием средств автоматизации обеспечивает проведение классификации информационных систем в установленном порядке.

4.10. Оператор при создании и эксплуатации информационных систем персональных данных как с использованием средств автоматизации, так и без использования средств автоматизации принимает все необходимые организационные и технические меры, обеспечивающие выполнение установленных действующим законодательством требований к обработке персональных данных.

4.11. Оператор при осуществлении обработки персональных данных обучающихся, работников без использования средств автоматизации выполняет следующие требования.

4.11.1. При ведении журналов (реестров, книг, иных документов), содержащих персональные данные обучающихся, работников, необходимые для организации образовательного процесса, Оператор соблюдает следующие условия:

- необходимость ведения такого журнала (реестра, книги, иных документов) предусматривается приказом Оператора, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги, иных документов), сроки обработки персональных данных;

- копирование содержащейся в таких журналах (реестрах, книгах, иных документах) информации не допускается, за исключением случаев, предусмотренных действующим законодательством.

4.11.2. Обработка персональных данных, осуществляемая без использования средств автоматизации, осуществляется таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

4.11.3. Обеспечивается раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

4.11.4. При хранении материальных носителей соблюдаются условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

4.11.5. Уточнение персональных данных обучающихся, работников при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

5. Права обучающихся, работников при обработке Оператором персональных данных

5.1. В целях обеспечения защиты своих интересов, реализации прав и свобод в сфере персональных данных, регламентированных действующим законодательством обучающиеся, их законные представители, а также представители (работники) имеют право на:

- предоставление Оператором полной информации об их персональных данных и обработке этих данных;
- свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные обучающегося, работника за исключением случаев, предусмотренных федеральным законом;
- определение своих представителей для защиты своих персональных данных;
- требование уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;
- требование об извещении Оператором всех лиц, которым ранее были сообщены неверные или неполные персональные данные обучающегося, работника обо всех произведенных в них исключениях, исправлениях или дополнениях;

- обжалование действий или бездействия оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

Права обучающегося, представителя, законного представителя, работника на доступ к своим персональным данным ограничиваются в случаях, предусмотренных действующим законодательством

5.2. От имени обучающихся, не достигших возраста 18 лет (не являющихся дееспособными), либо не признанных дееспособными в порядке, установленном Гражданским кодексом РФ права, указанные в п. 5.1. а также иные права и обязанности, установленные в настоящем положении, осуществляют законные представителя (родители, опекуны, попечители).

6. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

6.1 Лица, виновные в нарушении установленных требований в сфере обработки персональных данных, несут предусмотренную законодательством Российской Федерации ответственность.

6.2. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, законодательством, а также требований к защите персональных данных подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

6.3. Сотрудники Оператора, получившие в установленном порядке доступ к персональным данным, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных обучающихся, работников привлекаются к ответственности, предусмотренной действующим законодательством.

7. Заключительные положения

Настоящее Положение вступает в законную силу с момента утверждения его руководителем Оператора и действует до утверждения нового положения.

Приложение № 2 к приказу от 29.08.2022г. № 263

Директору МАОУ «ООШ № 280»

Е.П. Пятницкой

от

_____

_____

_____,

(фамилия, имя, отчество родителя (законного представителя))

Паспорт_____ №_____
выдан «__» _____ 20___ года
_____

_____

_____,

кем выдан документ

проживающего(ей) по адресу: п. Оленья Губа,

ул. _____,
д. ____, кв. _____,

контактный телефон: _____

СОГЛАСИЕ

на обработку персональных данных учащегося

Я, _____,

(фамилия, имя, отчество родителя (законного представителя))

в соответствии с пунктом 1 статьи 6 и статьей 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» своей волей и в своих интересах даю согласие ***Муниципальному автономному общеобразовательному учреждению «Основная общеобразовательная школа № 280» п. Оленья Губа имени Героя Российской Федерации Дениса Александровича Опарина (МАОУ «ООШ № 280»)***, зарегистрированному по адресу: Мурманская обл., п. Оленья Губа, ул. Строителей, д. 26/1, ОГРН 1025100748804, ИНН 5113100478, на обработку персональных данных моего ребенка,

_____,

(фамилия, имя, отчество ребенка)

«___» _____20____ года рождения, в объеме:

– фамилия, имя, отчество, дата и место рождения;
– пол;
– гражданство;
– адреса фактического места проживания и регистрации по местожительству;
– почтовые и электронные адреса;
– номера телефонов;
- СНИЛС;
- паспорт (свидетельство о рождении);
– сведения о родителях, законных представителях (фамилия, имя, отчество, дата и место рождения, пол, гражданство, место работы, должность, адреса, номера телефонов, СНИЛС, кем приходится ребенку);

– сведения о семье (категория семьи для оказания помощи и отчетности по социальному статусу контингента, реквизиты документов, подтверждающих право на льготы, гарантии и компенсации по основаниям, предусмотренным законодательством, – родители-инвалиды, неполная семья, многодетная семья, ребенок-сирота);

– сведения об образовании (форма получения образования, расписание занятий, выбор иностранного языка, предметов для профильного обучения и сдачи экзаменов, посещаемость занятий, оценки по предметам, результаты промежуточных и итоговых аттестаций, участия в олимпиадах, конкурсах и других мероприятиях, информация о внеучебной деятельности, продолжении обучения и трудоустройстве после отчисления из МАОУ «ООШ № 280»);

– сведения о личных качествах, поведении, результаты социально-психологического и других видов тестирования;

– сведения о состоянии здоровья (группа здоровья, инвалидность, хронические заболевания, прививки);

– информация, указанная в личном деле, портфолио учащегося;

– фотографии;

в целях:

– обеспечения соблюдения требований Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» и иных нормативных правовых актов сферы образования;

– безопасности и охраны здоровья учащегося;

– размещения фотографий на сайте школы;

– заполнения базы данных автоматизированных информационных систем: АИС «Электронная школа», ФИС ФРДО, РБД ГИА;

– индивидуального учета результатов освоения учащимися образовательных программ, хранения архивов данных об этих результатах на бумажных и/или электронных носителях.

Под обработкой необходимо понимать: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение, обезличивание, блокирование, уничтожение, хранение данных при автоматизированной и без использования средств автоматизации обработке.

Обязуюсь сообщать МАОУ «ООШ № 280» об изменении персональных данных

_____

(фамилия, имя, отчество ребенка)

в течение месяца после того, как они изменились.
Об ответственности за предоставление недостоверных персональных данных предупрежден (а).
Подтверждаю, что ознакомлен (а) с документами МАОУ «ООШ № 280», устанавливающими порядок обработки персональных данных, а также с моими правами и обязанностями.
Предупрежден (а), что согласие на обработку персональных данных может быть отозвано мною путем направления МАОУ «ООШ № 280» письменного отзыва.

Настоящее согласие действует со дня его подписания на период обучения

_____

(фамилия, имя, отчество ребенка)

в МАОУ «ООШ № 280».

«____» _____20____г. _____ /_____/

(подпись) (фамилия, инициалы)

Согласие на обработку персональных данных воспитанников

Я, _____

(фамилия, имя, отчество)

зарегистрированный (-ая) по адресу: _____

(адрес регистрации по месту жительства)

_____

документ, удостоверяющий личность: _____

(вид, серия и номер, дата выдачи, наименование выдавшего органа)

_____

в соответствии с требованиями ст. 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» **даю согласие** ***Муниципальному автономному общеобразовательному учреждению «Основная общеобразовательная школа № 280» п. Оленья Губа имени Героя Российской Федерации Дениса Александровича Опарина (МАОУ «ООШ № 280») расположенному по адресу: Мурманская область, п. Оленья Губа, ул. Строителей, д. 25***
(наименование ОО, адрес осуществления образовательной организации)

на обработку моих персональных данных и персональных данных несовершеннолетнего ребенка:

_____

(фамилия, имя, отчество, год рождения ребенка)

которому являюсь _____

(мать, отец, законный представитель (указать тип))

в целях обеспечения наиболее полного исполнения образовательной организацией своих обязанностей, обязательств и компетенций, определенных Федеральным законом от 29.12.2012 №273-ФЗ «Об образовании в Российской Федерации», а также:

- обеспечения соблюдения законов и иных нормативных правовых актов;
- учету детей, подлежащих обязательному обучению в образовательном учреждении;
- соблюдения порядка и правил приема в образовательное учреждение;
- индивидуального учета результатов освоения учащимися образовательных программ, а также хранения в архивах данных об этих результатах на бумажных носителях и/или электронных носителях;
- учета реализации права учащихся на получение образования в соответствии с государственными стандартами в форме самообразования, семейного образования, на обучение в пределах этих стандартов по индивидуальным учебным планам;
- учета учащихся, нуждающихся в социальной поддержке и защите;
- учета учащихся, нуждающихся в особых условиях воспитания и обучения и требующих специального педагогического подхода, обеспечивающего их социальную реабилитацию, образование и профессиональную подготовку, содействие учащимися в обучении, трудоустройстве;
- обеспечения личной безопасности учащихся;
- соблюдения порядка и правил приема и отчисления в образовательную организацию;
- планирования, организации, регулирования и контроля деятельности образовательного учреждения в целях осуществления государственной политики в области образования.

Перечень персональных данных, в отношении которых Оператор может осуществлять обработку, указан в приложении к настоящему согласию.

Я даю согласие на осуществление следующих действий (операций) с моими персональными данными и персональными данными моего ребенка: сбор; систематизацию; накопление; хранение, в том числе на электронных носителях; обновление; изменение; использование; обезличивание; блокирование; уничтожение; передачу государственными муниципальным организациям в целях осуществления их полномочий, в том числе в организацию, обслуживающую автоматизированные информационные системы «Электронный детский сад», «Электронная школа»; распространение неограниченному кругу лиц путем размещения информации, включая фото и видеоматериалы с участием меня и моего ребенка, на официальных сайтах образовательной организации, органа, осуществляющего управление в сфере образования, Министерства образования и науки Мурманской области, Правительства Мурманской области.

Я проинформирован, что Оператор гарантирует обработку персональных данных в соответствии с действующим законодательством Российской Федерации как неавтоматизированными, так и автоматизированными способами с использованием следующих информационных систем: **автоматизированная информационная система «Электронный детский сад»**.

Указанные персональные данные могут быть использованы для наполнения регионального сегмента единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам, созданном в целях реализации положений Правительства Российской Федерации от 25.10.2014 № 2125-р «Об утверждении Концепции создания единой федеральной межведомственной системы учета контингента по основным образовательным программам и дополнительным общеобразовательным программам».

Данное согласие действует с момента его подписания до достижения целей обработки персональных данных или в течение срока хранения информации.

Я уведомлен(а) о своем праве отозвать настоящее согласие в любое время. Отзыв производится по моему письменному заявлению в порядке, определенном законодательством Российской Федерации.

Подтверждаю, что ознакомлен(а) с Положением о защите персональных данных в образовательной организации и положениями Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», права и обязанности в области защиты персональных данных мне разъяснены.

Об ответственности за достоверность представленных сведений предупрежден(а).

Дата заполнения «___» _____ 20__ г.

Подпись: _____ (_____)

Ф.И.О.

Приложение № 3 к приказу от 29.08.2022г. № 263

Дополнение

в договор оказания образовательных услуг

Раздел «Обработка персональных данных»

Заказчик (законный представитель) в целях выполнения настоящего договора предоставляет Исполнителю (образовательному учреждению) на срок действия настоящего договора персональные данные обучающегося, а именно: фамилия, имя, отчество; пол; дата рождения; место рождения; гражданство; адрес места жительства, номер домашнего телефона, сведения о состоянии здоровья, сведения о законных представителях, иные необходимые сведения.

Исполнитель обязуется:

- обеспечить обработку персональных данных Заказчика в строгом соответствии с действующим законодательством, иными нормативными правовыми актами Российской Федерации в сфере обработки персональных данных;

- прекратить обработку персональных данных по достижении целей их обработки и обеспечить их уничтожение в установленном порядке.

Заказчик (законный представитель) в целях обеспечения защиты своих интересов, реализации прав и свобод в сфере персональных данных, регламентированных действующим законодательством, имеет право на предоставление Исполнителем полной информации о своих персональных данных и обработке этих данных; свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные Заказчика; на определение своих представителей для защиты своих персональных данных; на требование об исключении или исправлении неверных или неполных персональных данных, а также данных обработанных с нарушением действующего законодательства, а также иные права, предусмотренные действующим законодательством.

Приложение 4

к приказу от29.08.2022 № 263

Перечень
сведений конфиденциального характера в МАОУ «ООШ№280»

1. Сведения об обучающемся, позволяющие идентифицировать его личность (персональные данные):

- фамилия, имя, отчество;
- пол;
- дата рождения;
- место рождения;
- гражданство;
- состав семьи;
- адрес места жительства, домашний и мобильный телефон;
- сведения о состоянии здоровья и иные медицинские сведения;
- сведения о законных представителях.

2. Сведения о работнике образовательной организации, позволяющие идентифицировать его личность (персональные данные):

- фамилия, имя, отчество;
- пол;
- дата рождения;
- место рождения;
- гражданство;
- образование, специальность;
- учёная степень;
- стаж работы;
- предыдущее место работы;
- состояние в браке;
- состав семьи;
- адрес места жительства и домашний телефон;
- сведения о заработной плате;
- отсутствия судимости;
- заболевания, затрудняющие выполнение работником трудовых функций;
- данные предварительных и периодических медицинских осмотров, иные медицинские данные;
- любые иные сведения, с которыми работник считает нужным ознакомить работодателя или в предоставлении которых работодателю возникла необходимость.

3. Тестовые задания и контрольные измерительные материалы для оценки уровня учебных достижений обучающихся, содержащиеся в банке тестовых заданий, за исключением переведенных в установленном порядке в открытый доступ, текущего календарного года на бумажных и электронных носителях.

4. Результаты текущей, промежуточной и итоговой аттестации обучающихся на бумажных и электронных носителях .

5. Сведения и промежуточные статистические данные о результатах проведения единого государственного экзамена.

6. Сведения, содержащие информацию о прохождении и решениях, принимаемых на промежуточных этапах рассмотрения аттестационных дел сотрудников.

7. Сведения и статистические данные о результатах оказания услуг в образовательной организации до момента их официального опубликования.

8. Сведения, содержащие данные по результатам внутреннего и внешнего контроля объёмов и качества образовательных услуг и служебным проверкам.

9. Сведения о плане финансово-хозяйственной деятельности образовательной организации, до момента его официального опубликования.

10. Сведения о финансовых операциях.

11. Сведения о состоянии банковских счетов.

12. Сведения о планах закупок и инвестициях до момента их официального опубликования.

13. Сведения о содержании и характере договоров, контрактов, соглашений, одной из сторон в которых выступает образовательная организация.

14. Сведения относительно оборудования помещений образовательной организации охранной и пожарной сигнализацией и места ее установления.

15. Сведения об объёмах поступающих средств (из бюджета, из внебюджетных фондов, от предпринимательской деятельности, от спонсоров и жертвователей) до момента их официального опубликования.

16. Сведения о деятельности конкурсных комиссий и об оценке конкурсных предложений до момента утверждения победителя конкурса.

17. Сведения, раскрывающие содержание плана гражданской обороны образовательной организации.

18. Сведения, раскрывающие вопросы защиты образовательной организации от чрезвычайных ситуаций техногенного характера и террористических проявлений.

19. Другие сведения, связанные с деятельностью образовательной организации, которые не составляют государственной тайны, и разглашение которых может привести к причинению вреда, повлечь материальные убытки и нанести вред его деловой репутации.

Приложение 5
к приказу от29.08.2022 № 263

Положение
об ответственности работников, допущенных к обработке персональных данных и иной конфиденциальной информации

1. Общая часть

Конституцией Российской Федерации установлено, что каждый гражданин имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту чести и доброго имени. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются (ст. 23, 24 Конституции РФ).

В целях защиты частной жизни личности в связи со сбором персональных данных определена юридическая ответственность за нарушение установленных законодательством правил работы с персональными данными.

2. Ответственность работников, допущенных к обработке персональных данных

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами (ст. 90 ТК).

2.1. Дисциплинарная ответственность

На лицо, ненадлежащим образом относящееся к хранению и сбережению указанной информации, сведений, может быть наложено дисциплинарное взыскание.

Дисциплинарное взыскание может быть наложено на лицо, обязанное должным образом хранить и беречь информацию, касающуюся персональных данных работника, но в результате ненадлежащего хранения допустившего ее порчу или утрату.

Дисциплинарная ответственность предусмотрена трудовым законодательством (ст. 192-195 ТК РФ).

За совершение дисциплинарного проступка, т.е. неисполнение или ненадлежащее исполнение работником по его вине возложенных на него трудовых обязанностей (в том числе, применительно к рассматриваемой ст. 90 ТК РФ, это могут быть обязанности соблюдения установленного порядка со сведениями конфиденциального характера), работодатель вправе применить предусмотренные ст. 192 ТК дисциплинарные взыскания (замечание, выговор, увольнение по соответствующим основаниям) в порядке, установленном статьей 193 ТК РФ.

За разглашение охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с выполнением им своих трудовых обязанностей, может последовать расторжение трудового договора (см. п.п. "в" п. 6 ст. 81 ТК). Кроме того, на работников, разгласивших служебную или коммерческую тайну вопреки трудовому договору, может быть возложена обязанность возместить причиненные этим убытки (см. ст. 8, ч. 2 ст. 139 ГК РФ; п. 7 ч. 1 ст. 243 ТК).

2.2. Административная ответственность

В соответствии со ст. 13.11 КоАП РФ, предусматривающей ответственность за нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) накладывается административное взыскание. Нарушение данной нормы влечет за собой предупреждение или наложение штрафа в соответствии с законодательством РФ. В соответствии со ст. 13.14 КоАП РФ разглашение информации с ограниченным доступом лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, влечет за собой наложение административного штрафа на граждан в размере от 500 до 1 тысячи рублей; на должностных лиц - от 4 тысяч до 5 тысяч рублей (в ред. Федерального закона от 22.06.2007 N 116-ФЗ).

2.3. Гражданско-правовая ответственность

Гражданский кодекс предусматривает защиту нематериальных благ граждан, включая неприкосновенность частной жизни, личную и семейную тайну, деловую репутацию и др. Соответственно устанавливаются формы гражданско-правовой ответственности в виде денежной компенсации за причиненный моральный вред, обязанности опровержения сведений, порочащих честь, достоинство или деловую репутацию гражданина (работника) и т.п. (ст.ст. 150, 151, 152 ГК).

2.4. Уголовная ответственность

Уголовным кодексом РФ предусматривается уголовная ответственность: за злоупотребления и незаконные действия с информационными данными о частной жизни (ст. 137 УК), за неправомерный отказ должностного лица в предоставлении документов и материалов, непосредственно затрагивающих права и свободы гражданина, если эти деяния причинили вред правам и законным интересам граждан (в т.ч. работникам) (ст. 140 УК).

Так, ст. 137 Уголовного кодекса РФ гласит:

"1. Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации, если эти деяния совершены из корыстной или иной личной заинтересованности и причинили вред правам и законным интересам граждан, - наказывается штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов, либо исправительными работами на срок до одного года, либо арестом на срок до четырех месяцев.

2. Те же деяния, совершенные лицом с использованием своего служебного положения, - наказываются штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от пяти до восьми месяцев, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от четырех до шести месяцев".

Согласно ст. 272 УК РФ неправомерный доступ к охраняемой законом компьютерной информации, т.е. информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло за собой уничтожение, блокирование, модификацию либо копирование информации, наказывается штрафом в размере от 200 до 500 минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от 2 до 5 месяцев, либо исправительными работами на срок от 6 месяцев до одного года, либо лишением свободы на срок до двух лет (ч. 1). То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, наказывается штрафом в размере от 500 до 800 минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от 5 до 8 месяцев, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от 3 до 6 месяцев, либо лишением свободы на срок до 5 лет (ч. 2).

Приложение № 6 к приказу от 29.08.2022г. № 263

Директору МАОУ «ООШ № 280»
Е.П. Пятницкой

_____
_____
_____
(фамилия, имя, отчество)

паспорт:

_____

выдан:

_____
_____
_____

дата выдачи:

_____

зарегистрированного(ой) по адресу:

_____
_____
_____

СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Настоящим я,

_____,
(фамилия, имя, отчество)

в соответствии с пунктом 1 статьи 6 и статьей 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и главы 14 Трудового кодекса Российской Федерации представляю Работодателю (оператору):
Муниципальному автономному общеобразовательному учреждению «Основная общеобразовательная школа № 280» п. Оленья Губа имени /Героя Российской Федерации Дениса Александровича Опарина (МАОУ «ООШ № 280»), ИНН 5113100478 , ОГРН 1025100748804, зарегистрированному по адресу: ***184676, Мурманская область, п. Оленья Губа, ул. Строителей, д. 26/1,*** свои персональные данные в целях обеспечения соблюдения законов и иных нормативно-правовых актов при содействии в трудоустройстве, получении образования и продвижения по службе, обеспечения личной безопасности, текущей трудовой деятельности, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

Моими персональными данными является любая информация, относящаяся ко мне как к физическому лицу (субъекту персональных данных), указанная в трудовом договоре, личной карточке работника (унифицированная форма Т-2), трудовой книжке и полученная в течение срока действия настоящего трудового договора, в том числе: мои фамилия, имя, отчество, год, месяц, дата и место рождения, гражданство, документы, удостоверяющие личность, идентификационный номер налогоплательщика, номер страхового свидетельства государственного пенсионного страхования, адреса фактического места проживания и регистрации по местожительству, почтовые и электронные адреса, номера телефонов, фотографии, сведения об образовании, профессии, специальности и квалификации, сведения о наличии (или отсутствии) судимостей, семейном положении и составе семьи, сведения о состоянии здоровья, сведения об имущественном положении, доходах, задолженности, занимаемых ранее

должностях и стаже работы, воинской обязанности; сведения о трудовом договоре и его исполнении (занимаемые должности, существенные условия труда, сведения об аттестации, повышении квалификации и профессиональной переподготовке, поощрениях и наказаниях, видах и периодах отпуска, временной нетрудоспособности, социальных льготах, командировании, рабочем времени и пр.), а также о других договорах (индивидуальной, коллективной материальной ответственности, ученических, оказания услуг и т. п.), заключаемых при исполнении трудового договора; сведения о заработной плате, сведения о награждении государственными наградами Российской Федерации, присвоении почетных, воинских и специальных званий; сведения, необходимые для предоставления Работнику гарантий и компенсаций, установленных действующим законодательством (документы о составе семьи, о состоянии здоровья членов семьи, о беременности работницы, о возрасте малолетних детей, о донорстве и т.п.).

Своей волей и в своих интересах выражаю согласие на осуществление Работодателем (оператором) любых действий в отношении моих персональных данных, которые необходимы или желаемы для достижения указанных целей, в том числе выражаю согласие на обработку без ограничения моих персональных данных, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в т. ч. передачу), обезличивание, блокирование, уничтожение персональных данных при автоматизированной и без использования средств автоматизации обработке; запись на электронные носители и их хранение; размещение фотографии на сайте школы; заполнение базы данных автоматизированных информационных систем: АИС «Электронная школа», АИС «Электронный детский сад», РБД ГИА; предоставление информации в государственные органы Российской Федерации в порядке, предусмотренном действующим законодательством; передачу Работодателем (оператором) данных и соответствующих документов, содержащих персональные данные, третьим лицам: налоговым органам, в отделения Пенсионного фонда, Фонда социального страхования, в медицинские учреждения, военкомат, банку *ОАО Сбербанк* - в рамках зарплатного проекта; хранение моих персональных данных в течение 75 лет, содержащихся в документах, образующихся в деятельности Работодателя (оператора), согласно части 1 статьи 17 Закона от 22 октября 2004 г. № 125-ФЗ «Об архивном деле в Российской Федерации», а также при осуществлении любых иных действий с моими персональными данными, указанными в трудовом договоре и полученными в течение срока действия трудового договора, в соответствии с требованиями действующего законодательства РФ и Закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Настоящее согласие на обработку персональных данных действует с момента представления бессрочно и может быть отозвано мной при представлении Работодателю (оператору) заявления в простой письменной форме в соответствии с требованиями законодательства Российской Федерации.

Обязуюсь сообщать *в пятидневный срок* об изменении места жительства, контактных телефонов, паспортных, документных и иных персональных данных. Об ответственности за достоверность представленных персональных сведений предупрежден(а).

Подтверждаю, что ознакомлен (а) с документами МАОУ «ООШ № 280», устанавливающими порядок обработки персональных данных, а также с моими правами и обязанностями.

«____» _____ 20__ г. _____ _____

дата подпись фамилия, инициалы

Соглашение (обязательство) о неразглашении персональных данных работников

Я,

_____,
(Фамилия, имя, отчество)

паспорт: _____, дата выдачи: _____

выдан:_____

_____
(паспортные данные)

работающий(ая) в ***Муниципальном автономном общеобразовательном учреждении «Основная общеобразовательная школа № 280» п. Оленья Губа имени Героя Российской Федерации Дениса Александровича Опарина (МАОУ «ООШ № 280»)***
(наименование организации)

в должности _____

понимаю, что в соответствии с трудовым договором, должностной инструкцией получаю доступ к персональным данным физических лиц: ***работников МАОУ «ООШ № 280»***.

Перечень персональных данных работников: фамилия, имя, отчество, год, месяц, дата и место рождения, гражданство, документы, удостоверяющие личность, идентификационный номер налогоплательщика, номер страхового свидетельства государственного пенсионного страхования, адреса фактического места проживания и регистрации по местожительству, почтовые и электронные адреса, номера телефонов, фотографии, сведения об образовании, профессии, специальности и квалификации, сведения о наличии (или отсутствии) судимостей, семейном положении и составе семьи, сведения о состоянии здоровья, сведения об имущественном положении, доходах, задолженности, занимаемых ранее должностях и стаже работы, воинской обязанности; сведения о трудовом договоре и его исполнении (занимаемые должности, существенные условия труда, сведения об аттестации, повышении квалификации и профессиональной переподготовке, поощрениях и наказаниях, видах и периодах отпуска, временной нетрудоспособности, социальных льготах, командировании, рабочем времени и пр.), а также о других договорах (индивидуальной, коллективной материальной ответственности, ученических, оказания услуг и т. п.), заключаемых при исполнении трудового договора; сведения о заработной плате, сведения о награждении государственными наградами Российской Федерации, присвоении почетных, воинских и специальных званий; сведения, необходимые для предоставления гарантий и компенсаций, установленных действующим законодательством (документы о составе семьи, о состоянии здоровья членов семьи, о беременности работницы, о возрасте малолетних детей, о донорстве и т.п.).

Я также понимаю, что во время исполнения своих обязанностей мне предстоит заниматься сбором, систематизацией, накоплением, хранением, уточнением (обновлением, изменением), использованием, распространением (в т. ч. передачей), обезличиванием, блокированием, уничтожением персональных данных физических лиц при автоматизированной и без использования средств автоматизации обработке; записью на электронные носители и их хранением; размещением информации на сайте школы; заполнением базы данных автоматизированных информационных систем: АИС «Электронная школа», АИС «Электронный детский сад», РБД ГИА; предоставлением информации в государственные органы Российской Федерации в порядке, предусмотренном действующим законодательством; передачей данных и

соответствующих документов, содержащих персональные данные, третьим лицам: налоговым органам, в отделения Пенсионного фонда, Фонда социального страхования, в медицинские учреждения, военкомат, банку *ОАО Сбербанк* - в рамках зарплатного проекта.

Я обязуюсь хранить в тайне известные мне персональные данные работников, не использовать их персональные данные с целью получения выгоды, соблюдать установленный Положением об обработке персональных данных в МАОУ «ООШ № 280», порядок передачи третьим лицам сведений, составляющих персональные данные работников, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей; выполнять требования нормативных правовых актов, регламентирующих вопросы обработки персональных данных, информировать руководителя организации о фактах нарушения порядка обращения с персональными данными, о ставших мне известным попытках несанкционированного доступа к информации.

Я обязуюсь соблюдать правила пользования документами, порядком их учета и хранения, обеспечивать в процессе работы сохранность информации, содержащейся в них, от посторонних лиц, знакомиться только с теми служебными документами, к которым получаю доступ в силу исполнения своих служебных обязанностей.

Я понимаю, что разглашение информации, содержащей персональные данные, может нанести прямой или косвенный ущерб физическим лицам. В связи с этим даю обязательство при обработке персональных данных работников соблюдать все описанные в Федеральном законе от 27.07.2006 г. № 152-ФЗ «О персональных данных», постановлении Правительства РФ от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и других нормативных актах, требования.

Я предупрежден(а) о том, что в случае разглашения мной персональных данных работников или их утраты я несу ответственность в соответствии с действующим законодательством РФ.

С Положением об обработке персональных данных и Положением об ответственности работников, допущенных к обработке персональных данных и иной конфиденциальной информации в МАОУ «ООШ № 280» ознакомлен(а).

«____» _____ 20__ г. _____ _____

дата подпись фамилия, инициалы

Соглашение (обязательство) о неразглашении персональных данных учащихся, воспитанников, родителей (законных представителей)

Я,

_____,
(Фамилия, имя, отчество)

паспорт: _____, дата выдачи: _____

выдан:_____

_____
(паспортные данные)

работающий(ая) в ***Муниципальном автономном общеобразовательном учреждении «Основная общеобразовательная школа № 280» п. Оленья Губа имени Героя Российской Федерации Дениса Александровича Опарина (МАОУ «ООШ № 280»)***
(наименование организации)

в должности _____

понимаю, что в соответствии с трудовым договором, должностной инструкцией получаю доступ к персональным данным физических лиц: ***учащихся, воспитанников МАОУ «ООШ №280», родителей (законных представителей)***.

Перечень персональных данных учащихся, воспитанников: фамилия, имя, отчество, дата и место рождения; пол; гражданство; адреса фактического места проживания и регистрации по местожительству; почтовые и электронные адреса; номера телефонов; СНИЛС; паспорт (свидетельство о рождении), сведения о семье (категория семьи для оказания помощи и отчетности по социальному статусу контингента, реквизиты документов, подтверждающих право на льготы, гарантии и компенсации по основаниям, предусмотренным законодательством, – родители-инвалиды, неполная семья, многодетная семья, ребенок-сирота); сведения об образовании (форма получения образования, образовательная программа, расписание занятий, режим пребывания, выбор иностранного языка, предметов для профильного обучения и сдачи экзаменов, посещаемость занятий, оценки по предметам, результаты промежуточных и итоговых аттестаций, участия в олимпиадах, конкурсах и других мероприятиях, информация о внеучебной деятельности, продолжении обучения и трудоустройстве после отчисления из МАОУ «ООШ № 280»); сведения о личных качествах, поведении, результаты социально-психологического и других видов тестирования; сведения о состоянии здоровья (группа здоровья, инвалидность, хронические заболевания, прививки); информация, указанная в личном деле, портфолио учащегося; фотографии, видеоматериалы.

Перечень персональных данных родителей (законных представителей): фамилия, имя, отчество, дата и место рождения, пол, гражданство, место работы, должность, адреса, номера телефонов, СНИЛС, кем приходится ребенку.

Я также понимаю, что во время исполнения своих обязанностей мне предстоит заниматься сбором, систематизацией, накоплением, хранением, уточнением (обновлением, изменением), использованием, распространением (в т. ч. передачей), обезличиванием, блокированием, уничтожением персональных данных физических лиц при автоматизированной и без использования средств автоматизации обработке; записью на электронные носители и их хранением; размещением информации на сайте школы; заполнением базы данных автоматизированных информационных систем: АИС «Электронная школа», АИС «Электронный

детский сад», РБД ГИА; ФИС ФРДО в целях обеспечения соблюдения требований Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» и иных нормативных правовых актов сферы образования.

Я обязуюсь хранить в тайне известные мне персональные данные учащихся, родителей (законных представителей) учащихся, не использовать их персональные данные с целью получения выгоды, соблюдать установленный Положением об обработке персональных данных в МАОУ «ООШ № 280», порядок передачи третьим лицам сведений, составляющих персональные данные учащихся, родителей (законных представителей) учащихся, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей; выполнять требования нормативных правовых актов, регламентирующих вопросы обработки персональных данных, информировать руководителя организации о фактах нарушения порядка обращения с персональными данными, о ставших мне известным попытках несанкционированного доступа к информации.

Я обязуюсь соблюдать правила пользования документами, порядком их учета и хранения, обеспечивать в процессе работы сохранность информации, содержащейся в них, от посторонних лиц, знакомиться только с теми служебными документами, к которым получаю доступ в силу исполнения своих служебных обязанностей.

Я понимаю, что разглашение информации, содержащей персональные данные, может нанести прямой или косвенный ущерб физическим лицам. В связи с этим даю обязательство при обработке персональных данных работников соблюдать все описанные в Федеральном законе от 27.07.2006 г. № 152-ФЗ «О персональных данных», постановлении Правительства РФ от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и других нормативных актах, требования.

Я предупрежден(а) о том, что в случае разглашения мной персональных данных учащихся, воспитанников родителей (законных представителей) или их утраты я несу ответственность в соответствии с действующим законодательством РФ.

С Положением об обработке персональных данных и Положением об ответственности работников, допущенных к обработке персональных данных и иной конфиденциальной информации в МАОУ «ООШ № 280» ознакомлен(а).

«____» _____ 20__ г. _____ _____

дата подпись фамилия, инициалы

Приложение 7
к приказу от 29.08.2022 № 263

ПОЛОЖЕНИЕ
об обеспечении безопасности автоматизированной информационной системы
МАОУ «ООШ № 280»

1. Общие положения

Настоящее Положение определяет требования по обеспечению безопасности автоматизированной информационной системы (далее - АИС) МАОУ «ООШ № 280» (далее – Оператор).

АИС представляет собой IT-систему, предназначенную для автоматизации процессов формирования, обработки и анализа информации по основным направлениям деятельности Оператора.

Основными функциональными возможностями АИС Оператора являются:

- формирование, хранение и обновление сведений о структуре учебных подразделений Оператора;
- формирование, хранение и обновление сведений о преподавательском составе и сотрудниках учебных подразделений Оператора;
- формирование, хранение и обновление сведений об индивидуальных планах работы преподавательского состава;
- формирование, хранение и обновление сведений об учебном (учебно-производственном) плане Оператора;
- формирование, хранение и обновление сведений об учебной нагрузке преподавательского состава;
- формирование, хранение и обновление сведений о научной и учебно-методической продукции (методические рекомендации, учебные пособия, монографии, публикации) преподавательского состава;
- формирование, хранение и обновление сведений об обучающихся, проходящих обучение у Оператора;
- формирование, хранение и обновление сведений о результатах учебного процесса (итоги тестирования, экзаменов);
- аналитическая обработка информации о проведении учебного процесса как за отчётный период, так и о текущей деятельности учебных подразделений Оператора.

В качестве информации, подлежащей защите в АИС Оператора, рассматриваются:

- персональные данные преподавательского состава и сотрудников учебных подразделений;
- персональные данные обучающихся, проходящих и прошедших обучение;
- персональные данные административно-хозяйственных подразделений.

При обеспечении безопасности персональных данных в информационной системе Оператор руководствуется следующим: выбор средств защиты информации для системы защиты персональных данных; определение типа угроз безопасности персональных данных, актуальных для информационной системы; установление и обеспечение уровня защищённости персональных в информационной системе производится Оператором в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утверждённых постановлением Правительства РФ от 1 ноября 2012 г. N 1119.

Основными группами угроз, на противостояние которым направлены цели и требования безопасности, являются:

- угрозы, связанные с осуществлением несанкционированного доступа (ознакомления) с информацией, содержащей сведения о персональных данных работников и обучающихся, при ее обработке и хранении;
- угрозы, связанные с несанкционированным копированием (хищением) информации, содержащей сведения о персональных данных работников и обучающихся;
- угрозы, связанные с осуществлением доступа к информации, содержащей сведения о персональных данных работников и обучающихся, без разрешения на то ее владельца (субъекта персональных данных);
- угрозы, связанные с нарушением порядка доступа к информации, содержащей сведения о персональных данных работников и обучающихся, передаваемой заинтересованным лицам;
- угрозы, связанные с перехватом информации, содержащей сведения о персональных данных работников и обучающихся, из каналов передачи данных с использованием специализированных программно-технических средств;
- угрозы, связанные с потерей (утратой) информации, содержащей сведения о персональных данных работников и обучающихся, вследствие сбоев (отказов) программного и аппаратного обеспечения;
- угрозы, связанные с внедрением компьютерных вирусов и другого вредоносного программного обеспечения;
- угрозы, связанные с осуществлением несанкционированных информационных воздействий (направленных на «отказ в обслуживании» для сервисов, модификацию конфигурационных данных программно-аппаратных средств, подбор аутентификационной информации и т.п.).

Функциональные требования безопасности охватывают:
- требования к осуществлению аудита безопасности;
- требования к обеспечению подлинности субъектов обмена информацией;
- требования к криптографической поддержке;
- требования к защите информации, содержащей сведения о персональных данных работников и обучающихся;
- требования к идентификации и аутентификации пользователей АИС;
- требования к управлению безопасностью;
- требования к защите системы безопасности.

2. *Основные функциональные возможности АИС, связанные с обеспечением безопасности (защитой информации)*

2.1. Защита данных пользователя

АИС должна осуществлять функции и политику избирательного (дискреционного) управления доступом. Избирательное управление доступом должно предоставлять возможность ограничивать и контролировать доступ к системе и к информации, содержащей сведения о персональных данных.

Каждый Пользователь, пытающийся получить доступ к АИС, сначала должен проходить процедуру идентификации и аутентификации, а затем, при попытках получения доступа к активам, – авторизацию, т.е. проверку разрешений Пользователя по отношению к какому-либо защищаемому активу.

В АИС доступ к информации должен быть разрешен только уполномоченным на это Пользователям. Модель защиты АИС должна включать компоненты, которые реализуют контроль субъектов доступа, действий, предпринимаемых конкретной сущностью по отношению к объекту доступа.

Каждый объект доступа, представленный в АИС, должен быть однозначно ассоциирован с набором атрибутов безопасности, определяющих безопасность защищаемого объекта. Данный набор атрибутов должен формироваться при создании объекта и впоследствии может меняться. Изменение их значений должно быть обеспечено только Пользователям, имеющим статус владельца объекта, а также субъектам, которым предоставлены соответствующие полномочия.

Права доступа субъектов к объекту должны определяться посредством списка управления доступом. Список управления доступом должен включать перечень пользователей, которым разрешен доступ к объекту, а также набор допустимых над объектом действий.

2.2. Аудит событий безопасности

АИС должна обеспечивать набор средств аудита, предназначенных для мониторинга и обнаружения нежелательных условий, которые могут возникнуть, а также событий, которые могут произойти в системе. Мониторинг относящихся к безопасности событий должен позволять обнаруживать нарушителей безопасности, а также выявлять попытки несанкционированного доступа к АИС или доступа к защищаемой информации. В частности, определяя политику аудита, уполномоченный администратор АИС должен иметь возможность осуществлять аудит только необходимых типов событий безопасности, таких как неудачные попытки подключения пользователей к АИС. Запись результатов аудита событий безопасности должна осуществляться в журналы регистрации событий аудита, доступ к которому должен быть разрешен только уполномоченному администратору АИС. Просмотр журналов регистрации событий аудита должен выполняется с использованием средств АИС (специализированных инструментальных средств). Данные средства должны предоставлять возможность мониторинга и регистрации только тех событий аудита, которые удовлетворяют заданным критериям, что позволит ограничить объем данных, собираемых о событиях безопасности.

2.3. Идентификация и аутентификация

АИС должна требовать, чтобы все субъекты доступа уникально идентифицировались и аутентифицировались при доступе к АИС с помощью ввода идентификатора и пароля. Идентификация и аутентификация должны осуществляться до выполнения субъектом доступа каких-либо действий. АИС должна поддерживать аутентификацию Пользователей вместе с их авторизацией. Предусматривается, что авторизация Пользователей представляет начальный уровень для разрешения доступа к локальным и сетевым ресурсам.

АИС должна обеспечивать хранение паролей в преобразованном формате. АИС должна предоставлять средства усиления безопасности паролей через использование механизмов, позволяющих определить минимальную длину, время действия (минимальное и максимальное), задать требование уникальности (неповторяемости) и время смены пароля.

АИС должна предоставлять механизм блокирования учетной записи пользователя после определенного количества попыток ввода неправильного имени и/или пароля пользователя до ее разблокирования администратором АИС или по истечении времени действия, заданного для счетчика блокировки.

2.4. Защита системы безопасности

АИС должна предоставлять ряд возможностей для обеспечения защиты системы безопасности. Изоляция процессов и поддержания домена безопасности должны обеспечивать безопасное выполнение функций системы безопасности АИС. Возможность осуществления периодического тестирования среды функционирования АИС (аппаратной части) и собственно самих функций системы безопасности АИС должно обеспечивать поддержание уверенности администратора АИС в целостности и корректности функционирования функций системы безопасности.

3. Основные функциональные возможности повышения надежности

АИС должна обеспечивать надежную защиту данных от непредвиденных сбоев или отказов системы, обеспечивая следующие возможности по повышению надежности.

3.1. Резервное копирование данных

В АИС должны входить стандартные средства предотвращения потери данных и их восстановления в случае возможных сбоев. Имеющиеся средства резервного копирования должны предоставлять Пользователям возможность выбора различных стратегий резервного

копирования, обеспечивающих необходимый уровень защиты данных в случае возникновения сбоев в работе системы, при этом Пользователям должна предоставляться возможность выполнения резервного копирования данных на несъемные и съемные устройства хранения.

3.2. Восстановление системы

Функциональные возможности восстановления системы должны позволять возвращать АИС в состояние, предшествующее сбою. При этом в АИС не должно происходить потери (либо потери должны быть минимальны) и искажения данных.

3.3. Средства администрирования, управления и поддержки

В состав АИС должны быть интегрированы графические средства администрирования и/или утилиты командной строки, обеспечивающие эффективное полномасштабное и гибкое управление (в том числе мониторинг).

4. Среда безопасности АИС

4.1. Модели угроз, характерные для АИС

4.1.1. Осуществление несанкционированного ознакомления с персональными данными работников и обучающихся.

Источники угрозы – внешний злоумышленник.

Способ (метод) реализации угрозы – перехват информации из каналов передачи данных с использованием специализированных программно-технических средств.

Используемые уязвимости – возможные недостатки механизмов защиты информации при ее передаче по каналам передачи данных, связанные с возможностью несанкционированного ознакомления с передаваемой информацией третьих лиц.

Вид информации, потенциально подверженной угрозе – персональные данные работников и обучающихся.

Нарушаемое свойство безопасности – конфиденциальность.

Возможные последствия реализации угрозы – нанесения морального и/или материального ущерба лицу, фигурирующему в перехваченной информации. Нанесение косвенного материального ущерба образовательному учреждению.

4.1.2. Осуществление несанкционированного ознакомления с персональными данными работников и обучающихся и их модификация (в том числе подмена).

Источники угрозы – внешний злоумышленник.

Способ (метод) реализации угрозы – перехват информации из каналов передачи данных с использованием специализированных программно-технических средств; модификация (в том числе подмена) перехваченной информации и навязывание ложной информации.

Используемые уязвимости – недостатки механизмов защиты информации при ее передаче по каналам передачи данных, связанные с возможностью несанкционированного ознакомления и модификации (в том числе подмены) передаваемой информации.

Вид информации, потенциально подверженной угрозе – персональные данные работников и обучающихся.

Нарушаемые свойства безопасности – конфиденциальность, целостность.

Возможные последствия реализации угрозы – нанесения морального и/или материального ущерба лицу, фигурирующему в перехваченной информации из-за несанкционированного раскрытия конфиденциальной информации или распространения раскрытых данных. Нанесение косвенного материального ущерба образовательному учреждению.

4.1.3. Нарушение доступности, утрата или искажение предоставляемых персональных данных работников и обучающихся вследствие сбоев (отказов) программного и аппаратного обеспечения.

Источники угрозы – программное и аппаратное обеспечение.

Способ (метод) реализации угрозы – сбои (отказы) программного и аппаратного обеспечения.

Используемые уязвимости – недостатки механизмов обеспечения доступности требуемой информации, связанные с возможностью блокирования предоставления информации на недопустимое время.

Вид информации, потенциально подверженной угрозе – персональные данные работников и обучаемых.

Нарушаемое свойство безопасности – доступность, достоверность.

Возможные последствия реализации угрозы – нарушение со стороны образовательного учреждения взятых на себя обязательств по обработке персональных данных работников и обучающихся и может привести к прямому или косвенному материальному ущербу образовательному учреждению.

4.1.4. Нарушение согласованности данных в персональных данных работников и обучающихся вследствие сбоев (отказов) программного и аппаратного обеспечения, а также ошибок персонала образовательного учреждения.

Источники угрозы – программное и аппаратное обеспечение, персонал образовательного учреждения.

Способ (метод) реализации угрозы – сбои (отказы) программного обеспечения и ошибки персонала образовательного учреждения.

Используемые уязвимости – недостатки механизмов обеспечения согласованности данных в БД АИС, связанные с возможностью нарушения согласованности.

Вид информации, потенциально подверженной угрозе – персональные данные работников и обучающихся.

Нарушаемые свойства безопасности активов – достоверность, целостность.

Возможные последствия реализации угрозы – рассогласование в персональных данных работников и обучаемых, хранимых в БД АИС, что, в свою очередь, приведет к возможному нанесения морального и/или материального ущерба образовательному учреждению.

4.1.5. Осуществление доступа (ознакомления) с персональными данными обучающегося, хранимыми и обрабатываемыми в АИС, без согласия субъекта персональных данных или окончания срока действия такого согласия.

Источники угрозы – уполномоченные на доступ к персональным данным внутренние и внешние пользователи.

Способ (метод) реализации угрозы – осуществление доступа к персональным данным обучающихся с использованием штатных средств, предоставляемых программно-аппаратным обеспечением АИС.

Используемые уязвимости – недостатки механизмов защиты персональных данных обучающегося, связанные с возможностью доступа к ним без письменного согласия субъекта персональных данных или после окончания срока его действия.

Вид информации, потенциально подверженной угрозе – персональные данные обучающихся.

Нарушаемые свойства безопасности – конфиденциальность.

Возможные последствия реализации угрозы – несанкционированное ознакомление с персональными данными ведет к нанесению морального и/или материального ущерба обучающемуся из-за несанкционированного раскрытия конфиденциальной информации.

4.1.6. Внедрение в информационную систему образовательного учреждения вирусов и другого вредоносного программного обеспечения при взаимодействии с внешними системами, а также пользователями с носителей информации, используемых на автоматизированных рабочих местах.

Источники угрозы – внутренние пользователи и персонал образовательного учреждения, внешние системы.

Способ (метод) реализации угрозы – внедрение вирусов и другого вредоносного программного обеспечения при взаимодействии с внешними системами (файловый обмен, электронная почта и т.п.), а также при использовании съемных носителей информации на автоматизированных рабочих местах.

Используемые уязвимости – недостатки механизмов защиты информационной системы образовательного учреждения от внедрения вирусов и другого вредоносного программного обеспечения, связанные с возможностью внедрения вирусов и другого вредоносного программного обеспечения.

Вид информации, потенциально подверженной угрозе – программное обеспечение информационной системы образовательного учреждения.

Нарушаемое свойство безопасности активов – целостность.

Возможные последствия реализации угрозы – нарушение режимов функционирования информационной системы образовательного учреждения, потеря (утрата) и искажение информации, снижение уровня защищенности информационной системы образовательного учреждения. Ведет к возможному материальному ущербу образовательному учреждению.

4.1.7. Осуществление несанкционированных информационных воздействий (модификация конфигурационных данных программно-аппаратных средств, подбор аутентификационной информации и т.п.) на информационную систему образовательного учреждения, осуществляемых из внешних систем.

Источники угрозы – внешние злоумышленники, внешние системы.

Способ (метод) реализации угрозы – несанкционированные информационные воздействия с использованием специализированного программно-аппаратного обеспечения.

Используемые уязвимости – недостатки механизмов защиты информационной системы образовательного учреждения от несанкционированных внешних воздействий.

Вид информации, потенциально подверженной угрозе – программно-аппаратное обеспечение информационной системы образовательного учреждения.

Нарушаемые свойства безопасности активов – конфиденциальность, целостность.

Возможные последствия реализации угрозы – нарушение режимов функционирования информационной системы образовательного учреждения, снижение уровня защищенности информационной системы образовательного учреждения. Ведет к возможному материальному ущербу образовательному учреждению.

4.2. Политика и цели безопасности для АИС

АИС должна обеспечить следование приведенным ниже правилам безопасности:

1. Должна быть обеспечена регистрация и учет получения (включая указание срока действия) согласия обучающегося на обработку предоставленных им в образовательное учреждение своих персональных данных.
2. Должна быть обеспечена возможность надежного хранения персональных данных работников и обучающихся (в течение действия срока трудового договора и разрешения на обработку персональных данных соответственно).
3. Должна быть обеспечена возможность безопасного восстановления АИС после сбоев и отказов программного обеспечения и оборудования.
4. Должна быть обеспечена защита информации, составляющей персональные данные работников и обучающихся, при ее обработке, хранении и передаче специализированными средствами защиты.
5. Должно быть обеспечено наличие надлежащих, защищенных от несанкционированного использования, механизмов регистрации и предупреждения администратора АИС о любых событиях, относящихся к безопасности АИС.
6. Должно быть обеспечено наличие надлежащих и корректно функционирующих средств администрирования безопасности информационной системы образовательного учреждения, доступных только уполномоченным администраторам.
7. Должны быть предоставлены механизмы аутентификации, обеспечивающие адекватную защиту от прямого или умышленного нарушения безопасности нарушителями с низким потенциалом нападения.
8. Должны быть обеспечены механизмы генерации, надлежащего и защищенного распределения, уничтожения ключевой информации, а также механизмы шифрования, и формирования электронной цифровой подписи. Данные механизмы должны функционировать в соответствии с сертифицированными алгоритмами.

4.3. Политика и цели безопасности для среды функционирования АИС

Среда функционирования АИС должна обеспечить следование приведенным ниже правилам безопасности:

1. Должна быть обеспечена инженерно-техническая укреплённость объектов размещения системы обработки, хранения и передачи информации, содержащей сведения о персональных данных.
2. Объекты размещения системы обработки, хранения и передачи информации, содержащей сведения о персональных данных, должны быть оборудованы системой охранной сигнализации.
3. Должна быть исключена возможность несанкционированного физического доступа к программно-аппаратным элементам системы обработки, хранения и передачи информации, содержащей сведения о персональных данных, со стороны посторонних лиц.
4. На объектах системы обработки, хранения и передачи информации, содержащей сведения о персональных данных, должно быть обеспечено наличие и надлежащее использование средств антивирусной защиты, сертифицированных по требованиям безопасности. Должно быть обеспечено регулярное обновление антивирусных баз.
5. Объекты системы обработки, хранения и передачи информации, содержащей сведения о персональных данных, должно быть подключены к внешним вычислительным сетям общего пользования с использованием надлежащих средств межсетевого экранирования, сертифицированных по требованиям безопасности.
6. На объектах системы обработки, хранения и передачи информации, содержащей сведения о персональных данных, должно быть обеспечено отсутствие нештатных программных средств, не имеющих отношение к процессу функционирования образовательного учреждения.
7. Должны быть обеспечены установка, конфигурирование и управление программно-аппаратными средствами АИС в соответствии с руководствами и согласно оцененным конфигурациям.
8. Персонал, ответственный за администрирование АИС, должен быть благонадежным и компетентным, и руководствоваться в своей деятельности соответствующей документацией.

9. Уполномоченные на работу с АИС операторы должны быть благонадежными, руководствоваться в своей работе эксплуатационной документацией на АИС, а их совместные действия должны быть направлены исключительно на выполнение своих функциональных обязанностей.

Приложение 8
к приказу от29.08.2022 № 263

ПОЛОЖЕНИЕ
о парольной защите при обработке персональных данных и иной конфиденциальной информации

Данное Положение регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (учетных записей Пользователей) в информационных системах (АИС) МАОУ «ООШ № 280» (далее Оператора), а также контроль за действиями Пользователей и обслуживающего персонала при работе с паролями.

1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех АИС и контроль за действиями Пользователей и обслуживающего персонала при работе с паролями возлагается на сотрудников школы, работающих с автоматизированными информационными системами (АИС *или иного соответствующего подразделения (или уполномоченного лица) Оператора*) - администраторов парольной защиты.

2. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями ИС самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;
- личный пароль Пользователь не имеет права сообщать никому.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

3. В случае, если формирование личных паролей Пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на уполномоченных сотрудников отдела АИС (*или иного соответствующего подразделения (или уполномоченного лица) Оператора*). Для генерации «стойких» значений паролей могут применяться специальные программные средства. Система централизованной генерации и распределения паролей должна исключать возможность ознакомления самих уполномоченных сотрудников отдела АИС (*или иного соответствующего подразделения (или уполномоченного лица) Оператора*) с паролями других сотрудников подразделений Оператора.

4. При наличии технологической необходимости (в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п.) использования имен и паролей некоторых сотрудников (Пользователей) в их отсутствие, такие сотрудники обязаны сразу же после смены своих паролей передавать на хранение руководителю своего подразделения их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте. Опечатанные конверты с паролями Пользователей должны храниться в сейфе. Для опечатывания конвертов должны применяться личные печати владельцев паролей (при их наличии у Пользователей), либо печать отдела АИС (*или иного соответствующего подразделения (или уполномоченного лица) Оператора*).

5. Полная плановая смена паролей Пользователей должна проводиться регулярно, не реже одного раза в квартал *(или в иные установленные Оператором сроки)*.

6. Внеплановая смена личного пароля или удаление учетной записи Пользователя ИС в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться сотрудниками отдела АИС (*или иного соответствующего подразделения (или*

уполномоченного лица) Оператора) немедленно после окончания последнего сеанса работы данного Пользователя с системой.

7. Внеплановая полная смена паролей всех Пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) администраторов средств защиты и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой ИС.

8. В случае компрометации личного пароля Пользователя ИС должны быть немедленно предприняты меры в соответствии с п. 6 или п. 7 настоящего Положения в зависимости от полномочий владельца скомпрометированного пароля.

9. Хранение Пользователем своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у руководителя подразделения в опечатанном личной печатью конверте (возможно вместе с персональными ключевыми носителями и идентификатором Touch Memory).

10. Повседневный контроль за действиями Пользователей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на руководителей подразделений, периодический контроль – возлагается на сотрудников отдела АИС (*или иного соответствующего подразделения (или уполномоченного лица) Оператора*) – администраторов парольной защиты.

Приложение 9
к приказу от29.08.2022 № 263

Инструкция о применении средств антивирусной защиты информации

1. Термины и определения

В Инструкции о применении средств антивирусной защиты информации (далее - Инструкция) использованы следующие термины и определения:

Пользователи - должностные лица, а также все другие лица и организации, использующие в работе средства электронно-вычислительной техники.

Администраторы антивирусной защиты информации (далее -администраторы АВЗ) - должностные лица подразделений информационной безопасности (технических подразделений), назначенные ответственными за эксплуатацию средств антивирусной защиты информации и обеспечивающие организацию и эффективное использование системы антивирусной защиты информации.

Локально-вычислительная сеть (далее - ЛВС) - группа ЭВМ, а также периферийное оборудование, объединенные одним или несколькими автономными (неарендуемыми) высокоскоростными каналами передачи цифровых данных в пределах одного или нескольких близлежащих зданий.

Антивирусная защита информации - система организационно-технических мероприятий, требований и условий использования электронно-вычислительной техники, предназначенная для предотвращения заражения программными вирусами информационно-вычислительных ресурсов посредством применения средств антивирусной защиты информации.

Вредоносная программа - программа для электронно-вычислительных машин (ЭВМ), заведомо приводящая к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети.

Программные вирусы - разновидность вредоносных программ, отличительной особенностью которых является способность к размножению (саморепликации). В дополнение к этому они могут повреждать или полностью уничтожать данные, подконтрольные пользователю, от имени которого была запущена зараженная программа.

Информационно-техническая служба – структурное подразделение организации, ответственное за функционирование автоматизированных информационных систем и электронно-вычислительной техники. В небольших организациях на него могут быть возложены и функции службы информационной безопасности.

2. Общие положения

1. Настоящая Инструкция разработана в целях осуществления антивирусной защиты информации, содержащейся и обрабатываемой на рабочих станциях структурных подразделений организации, от несанкционированного копирования, модификации и разрушения данных, используемых в деятельности учреждения, а также нарушения работы используемого программного обеспечения при воздействии вирусов и других вредоносных программ посредством комплекса организационно-технических мероприятий по обеспечению информационной безопасности.

2. Настоящая Инструкция определяет порядок применения средств антивирусной защиты в структурных подразделениях, задачи, обязанности и права администраторов АВЗ, пользователей средств антивирусной защиты информации, порядок установки и применения

обновлений, подключения средств антивирусной защиты, а также порядок ликвидации последствий воздействия программных вирусов.

3. Требования настоящей Инструкции обязательны для выполнения всеми пользователями и администраторами АВЗ, а также иными лицами, использующими средства вычислительной техники.

4. Общее руководство обеспечением антивирусной защиты информации в осуществляется информационно-технической службой (далее - ИТС) и ответственным за информационную безопасность и техническую защиту информации ИТС.

5. Ответственный за информационную безопасность и техническую защиту информации ИТС осуществляет непосредственное руководство организацией работ по антивирусной защите информации в организации через сотрудников ИТС.

6. Практическое решение задач, связанных с организацией антивирусной защиты информации и применением средств антивирусной защиты информации в структурных подразделениях, осуществляется сотрудниками ИТС.

7. При возникновении ситуаций, не включенных в положения настоящей Инструкции, решение принимается администратором АВЗ по согласованию с ответственным за информационную безопасность и техническую защиту информации ИТС.

3. Порядок применения средств антивирусной защиты информации в образовательном учреждении

1. Средства антивирусной защиты информации должны устанавливаться на всех средствах вычислительной техники, эксплуатируемых в образовательной организации. При технологической необходимости на отдельные средства вычислительной техники средства антивирусной защиты информации могут не устанавливаться. Список таких исключений утверждается руководителем ИТС и пересматривается ежегодно.

2. Порядок применения средств антивирусной защиты информации устанавливается с учетом соблюдения следующих требований:

- обязательный входной контроль за отсутствием программных вирусов во всех поступающих на объект информатизации электронных носителях информации, информационных массивах, программных средствах общего и специального назначения;
- обязательная проверка всех электронных писем на предмет отсутствия программных вирусов;
- периодическая проверка на предмет отсутствия программных вирусов жестких магнитных дисков (не реже одного раза в неделю) и обязательная проверка съемных носителей информации перед началом работы с ними;
- внеплановая проверка жестких магнитных дисков и съемных носителей информации в случае подозрения на наличие программных вирусов;
- восстановление работоспособности программных средств и информационных массивов, поврежденных программными вирусами.

3. Уполномоченное лицо организации по антивирусной защите информации обеспечивает:

- управление конфигурацией и логической структурой всего программного обеспечения системы антивирусной защиты информации;
- управление установкой и обновлением лицензионных ключей средств антивирусной защиты информации;
- управление рассылкой и установкой обновлений баз средств антивирусной защиты информации;

- ограничение доступа пользователей на рабочих местах к настройкам установленных средств антивирусной защиты информации;

- настройку рассылки сообщений об обнаружении вирусов, о сбоях в работе средств антивирусной защиты и т.п.;

- удаленное решение проблем, возникающих в процессе использования средств антивирусной защиты информации.

4. Для рабочих станций и серверов, которые не имеют подключения к ЛВС, средства антивирусной защиты информации для них устанавливаются локально в порядке, определенном администратором АВЗ, с учетом требований настоящей Инструкции.

5. Инсталляция и настройка средств антивирусной защиты информации осуществляются в соответствии с программной и эксплуатационной документацией, поставляемой в комплекте с ними.

6. Копирование любой информации, переносимой с помощью любых съемных носителей информации, должно производиться только после проведения процедуры полного антивирусного контроля съемного носителя.

7. Антивирусная профилактика является необходимым элементом защиты информационных ресурсов учреждения от их модификации и уничтожения. Антивирусная профилактика состояния средств антивирусной защиты информации на серверах и рабочих станциях должна проводиться по согласованию с администраторами АВЗ в нерабочее время, за исключением внештатных ситуаций.

4. Порядок обновления баз данных средств антивирусной защиты информации

1. Своевременное обновление баз данных средств антивирусной защиты информации в структурных подразделениях является неотъемлемой частью обеспечения эффективной политики антивирусной защиты информации.

2. Обновление баз данных средств антивирусной защиты информации на рабочих станциях, установленных локально в структурных подразделениях, должно производиться не реже одного раза в неделю в порядке, устанавливаемом администратором АВЗ, с учетом требований настоящей Инструкции.

3. На рабочем месте администратора АВЗ могут быть установлены средства, позволяющие через ЛВС управлять компонентами системы антивирусной защиты, установленными на рабочих станциях и серверах в структурных подразделениях, а также проводить обновления баз средств антивирусной защиты информации. В случае если рабочая станция пользователя не подключена к ЛВС, обновление средств антивирусной защиты информации производится пользователем через съемные носители информации. Периодичность обновления определяется программными требованиями средств антивирусной защиты информации или устанавливается администратором АВЗ.

5. Обязанности, права и порядок назначения администраторов АВЗ

1. Администраторы АВЗ обязаны обеспечивать соблюдение в учреждении политики антивирусной защиты информации и выявление фактов заражения программными вирусами.

2. К основным задачам администратора АВЗ относятся организация процесса установки и обновления средств антивирусной защиты информации

на рабочих станциях пользователей и обеспечение технического сопровождения действий пользователей в случаях обнаружения программных вирусов, а также осуществление контроля за состоянием системы антивирусной защиты информации.

3. Администратор АВЗ несет ответственность: за своевременную установку средств антивирусной защиты информации;

- за эксплуатацию системы антивирусной защиты информации;
- за своевременное обновление лицензий на средства антивирусной защиты информации;
- за своевременное обновление баз данных средств антивирусной защиты информации.

4. Администратор АВЗ имеет право:

- вносить предложения по совершенствованию системы антивирусной защиты информации в структурных подразделениях образовательного учреждения;
- принимать участие в планировании мероприятий по антивирусной защите информации в организации и планировании оснащения средствами антивирусной защиты информации структурных подразделений;
- осуществлять контроль состояния средств антивирусной защиты информации в структурных подразделениях;
- проводить служебные проверки по фактам заражения программными вирусами автоматизированных систем обработки информации и средств вычислительной техники в структурных подразделениях образовательного учреждения;
- оказывать помощь в решении проблем, возникающих при эксплуатации средств антивирусной защиты информации в структурных подразделениях образовательного учреждения.

5. Назначение администраторов АВЗ организации осуществляется на основании приказа по образовательной организации с обязательным отражением обязанностей в должностной инструкции.

6. Обязанности администраторов АВЗ могут совмещать должностные лица, назначенные администраторами баз данных (автоматизированных информационных систем), специалисты ИТС. Администраторами АВЗ не могут быть должностные лица сторонних организаций. Должностные лица, исполняющие обязанности администраторов АВЗ, утверждается приказом руководителя образовательной организации.

7. Обязанности администраторов АВЗ организации другие лица могут исполнять только на основании приказа руководителя организации о временном исполнении обязанностей администратора АВЗ, в котором указан срок исполнения обязанностей администратора АВЗ.

6. Обязанности пользователей средств антивирусной защиты информации

1. Пользователь обязан изучить настоящую Инструкцию и ознакомиться с необходимостью несения ответственности за выполнение ее требований под роспись.

2. Пользователям запрещается:

- отключать средства антивирусной защиты информации во время работы;
- использовать средства антивирусной защиты информации, отличные от поддерживаемых ИТС, перечень которых доводится до сведения пользователей ИТС или администраторов АВЗ;
- без разрешения администратора ЛВС и администратора АВЗ копировать любые файлы, устанавливать и использовать любое программное обеспечение, не предназначенное для выполнения служебных задач.

3. Ввод информации с магнитных, оптических, магнитооптических и любых других съемных носителей информации неслужебного характера должен осуществляться пользователем только с разрешения администраторов ЛВС или администраторов АВЗ.

4. В случае появления подозрений на наличие программных вирусов в ЛВС пользователи должны немедленно проинформировать об этом администратора АВЗ. В случае выявления инцидентов (фактов и т.п.), связанных со сбоями в работе средств антивирусной защиты, пользователь обязан незамедлительно сообщить об этом ответственному за информационную безопасность и техническую защиту информации ИТС.

7. Порядок действий пользователей и администраторов АВЗ при обнаружении вирусов

1. Основными путями проникновения вирусов в информационно - вычислительную сеть организации являются: гибкие магнитные диски, компакт-диски, иные съемные накопители информации, электронная почта, файлы, получаемые из сети Интернет, ранее зараженные рабочие станции. В случае обнаружения программных вирусов при входном контроле отчуждаемых носителей информации, файлов или почтовых сообщений, поступивших в структурные подразделения, пользователь должен:

- приостановить процесс приема-передачи информации;
- сообщить администратору АВЗ или ответственному за информационную безопасность и техническую защиту информации ИТС о факте обнаружения программного вируса;
- принять по согласованию с администратором АВЗ меры по локализации и удалению программного вируса с использованием средств антивирусной защиты информации;
- сообщить о факте обнаружения программного вируса в структурное подразделение, из которого поступили зараженные съемные электронные носители информации, файлы или почтовые сообщения.

2. При обнаружении программных вирусов в процессе обработки информации пользователь обязан:

- немедленно приостановить все работы;
- сообщить администратору АВЗ или ответственному за информационную безопасность и техническую защиту информации ИТС о факте обнаружения программных вирусов;
- принять по согласованию с администратором АВЗ меры по локализации и удалению программного вируса с использованием средств антивирусной защиты информации.

3. Программные средства общего и специального назначения, используемые в структурных подразделениях для обработки информации, отнесенной к служебной тайне, в случае обнаружения программных вирусов подлежат обязательной переустановке с рабочих копий эталона.

4. При невозможности ликвидации последствий заражения программными вирусами администратору АВЗ необходимо:

- заархивировать зараженные файлы с внедренными программными вирусами и направить с приложением соответствующего сопроводительного документа в организацию, осуществляющую техническую поддержку эксплуатации средств антивирусной защиты информации;
- осуществить полную переустановку программного обеспечения на зараженном компьютере.

5. При получении информации о возможном нарушении либо выявлении факта нарушения требований настоящей Инструкции работа на рабочей станции данного пользователя незамедлительно блокируется по решению администратора АВЗ.

6. Все факты модификации и разрушения данных на серверах или рабочих станциях, заражение их вирусами, а также обнаружение других вредоносных программ классифицируются как значимые нарушения информационной безопасности и должны анализироваться посредством проведения служебного расследования, проводимого по приказу руководителя образовательного учреждения.

8. Ответственность за выполнение требований Инструкции

1. За нарушение настоящей Инструкции администратор АВЗ и пользователи несут ответственность, установленную действующим законодательством Российской Федерации и нормативными правовыми актами.

2. Руководители структурных подразделений несут ответственность за выполнение мероприятий по антивирусной защите информации на средствах вычислительной техники, эксплуатируемых подчиненными должностными лицами, и за ознакомление их (под роспись) с настоящей Инструкцией в своем структурном подразделении.

3. Непосредственную ответственность за соблюдение в повседневной деятельности установленных норм обеспечения антивирусной защиты информации на своих рабочих местах, в том числе за своевременное обновление антивирусных баз средств антивирусной защиты информации и получение новых лицензионных ключей, несут пользователи, за которыми закреплены средства вычислительной техники.

4. В случае нарушения требований настоящей Инструкции, связанных с применением пользователем средств антивирусной защиты информации, пользователь несет персональную ответственность, установленную действующим законодательством Российской Федерации и локальными нормативными актами образовательной организации.

5. Ответственность за выполнение требований настоящей Инструкции администраторами АВЗ несут непосредственно администраторы АВЗ и руководители подразделений, в которых работают администраторы АВЗ.

9. Порядок оснащения организации средствами антивирусной защиты информации

1. Оснащение средствами антивирусной защиты информации является видом материального обеспечения и осуществляется в образовательной организации централизованно.

2. Передача полученных средств антивирусной защиты на объекты, не входящие в состав организации, запрещена. За несанкционированное распространение средств антивирусной защиты информации виновные несут ответственность в соответствии с законодательством Российской Федерации.

Приложение 10
к приказу от29.08.2022 № 263

Регламент использования программного обеспечения

1. Общие положения

Настоящий Регламент распространяет своё действие на сотрудников МАОУ «ООШ №280», выполнение должностных обязанностей которых связано с использованием персональных компьютеров, и определяет их полномочия, обязанности и ответственность при использовании программного обеспечения.

Регламент является обязательным для выполнения всеми сотрудниками – пользователями образовательной организации. Настоящий Регламент может уточняться и дополняться в установленном порядке

2 Сокращения и понятия

В Регламенте используются следующие сокращения и понятия:

- ПК - персональный компьютер;
- ПО - программное обеспечение;
- ИР – информационные ресурсы;
- пользователь – сотрудник организации, выполнение должностных обязанностей которого связано с использованием ПК и ПО;
- администратор – сотрудник информационно-технической службы, ответственный за предоставление ПО и обеспечение работоспособности ПО, надежности ПО, сохранности и защиты информационных ресурсов.

3. Общие требования

Руководители структурных подразделений, пользователи и администраторы обязаны знать и выполнять нормативные правовые акты, затрагивающие вопросы легального использования ПО и ИР на которые распространяются авторские права, в части соблюдения требований и ограничений по использованию.

Руководители структурных подразделений в обязательном порядке организуют ознакомление пользователей с нормативными правовыми актами, указанными в настоящем Регламенте.

Использование ПО и ИР осуществляется на рабочем ПК пользователя. Ответственность за действия на компьютере другого человека, несет пользователь ПК на котором совершено это действие.

Работа пользователей отслеживается с помощью специального программного обеспечения удаленно, а также периодическим аудитом ПО установленного на ПК пользователя

4. Требования к пользователю

Данный раздел отражает полномочия, обязанности и ограничения прав пользователей ПК и ПО.

Пользователю запрещается:

- использовать ИР, на которые распространяются права правообладателя без соответствующих полномочий на использование ИР;
- допускать к работе посторонних лиц;
- строго запрещается использовать ПО без соответствующей лицензии, в любых вариантах, противоречащих законодательству;

- загружать, самостоятельно устанавливать прикладное, операционное, сетевое и другие виды программного обеспечения, а также осуществлять обновления, если эта работа не входит в его должностные обязанности;
- использовать любые ИР в не служебных целях;
- строго запрещается использовать ПО, относящееся к числу свободно распространяемых, но не используемых в образовательной организации.

Пользователь обязан знать и уметь пользоваться ПО.

Пользователь обязан информировать администратора о любых нарушениях при использовании ПО и ИР.

Пользователь имеет право оспаривать решение администратора через своего непосредственного руководителя, который в свою очередь обращается в информационно-техническую службу. Если обе стороны не могут прийти к консенсусу, тогда вопрос рассматривает руководитель образовательного учреждения или уполномоченное им лицо.

5. Требования к администратору

Данный раздел отражает функциональные полномочия и обязанности администратора, обеспечивающего использование ПО и ИР.

Администратор обязан:

- производить обеспечение доступа к ИР и установку ПО в порядке установленном законодательством РФ, иными нормативными правовыми актами;
- знать и правильно использовать аппаратно - программные средства для обеспечения стабильной и надежной работы ПО и возможности использования ИР;
- оказывать методическую и консультационную помощь пользователям по вопросам, входящим в его компетенцию, в соответствии с утверждённым графиком работы;
- постоянно вести учет и анализ использования ПО и ИР по каждому пользователю, предоставлять этот отчет руководству;
- информировать руководителей структурных подразделений о любых нарушениях требований настоящего Регламента;
- обеспечить сбор данных о необходимости использования типов ПО и ИР в подразделениях образовательного учреждения;
- обеспечивать использование в организации лицензионного ПО и вести его соответствующий учёт по каждому структурному подразделению.

Администратор имеет право:

при обнаружении использования ПО и ИР с отступлениями от Регламента блокировать работу пользователя до момента вынесения окончательного решения руководителем образовательной организации.

6. Порядок предоставления ПО и ИР

Порядок предоставления ПО и ИР:

- ПО и ИР пользователю предоставляются исходя из служебной необходимости, на основании служебной записки на имя руководителя образовательной организации от руководителя структурного подразделения;
- Руководитель организации на основании служебной записки даёт поручение администратору, обеспечивающему использование ПО и ИР во взаимодействии с руководителем структурного подразделения образовательного учреждения, где планируется размещение соответствующего ПО и ИР, назначить права конкретному пользователю по использованию ПО и ИР.
- После этого администратор, обеспечивающий использование ПО и ИР, осуществляет обеспечение пользователя необходимыми ПО и ИР, с отметкой в журнале установленной формы.

- Изменения в порядке и перечне используемого ПО и ИР также производятся на основании служебной записки на имя руководителя образовательной организации.

7. Порядок разрешения споров

В случае возникновения претензий или вопросов, касающихся конкретного случая использования ПО и ИР, невозможности продолжения работы в соответствии со своими обязанностями, пользователь обращается к администратору. Если претензию не удаётся разрешить двум сторонам, тогда вопрос рассматривает руководитель образовательной организации или уполномоченное им лицо.

Приложение 11
к приказу от 29.08.2022 № 263

Регламент
использования электронной почты в образовательной организации

1. Общие положения

Настоящий Регламент разработан в целях установления единого порядка использования корпоративной электронной почты (далее - ЭП) образовательной организации, обязательной для использования в работе работниками МАОУ «ООШ № 280».

Настоящий Регламент призван обеспечить бесперебойную работу и эффективное использование ЭП в интересах деятельности образовательной организации.

Настоящий Регламент не определяет порядок работы с документами, направляемыми и получаемыми по ЭП.

Каждый работник образовательной организации, имеющий личный почтовый ящик корпоративной ЭП, обязан использовать его в рамках выполнения своих трудовых обязанностей.

Вся информация и сообщения, которые были созданы, отправлены, приняты или сохранены посредством корпоративной ЭП образовательной организации, принадлежит образовательной организации, за исключением случаев, предусмотренных законодательством Российской Федерации.

В пределах функционирования корпоративной ЭП обеспечивается конфиденциальность почтовых сообщений и информации о пользователях ЭП, кроме информации из адресной книги и за исключением случаев, предусмотренных законодательством Российской Федерации.

2. Характеристика корпоративной электронной почты образовательной организации

Корпоративная ЭП образовательной организации состоит из следующих компонентов:

- Адресная книга, содержащая информацию о пользователях. Информация Адресной книги доступна всем зарегистрированным пользователям.
- Личные папки - локальные дисковые хранилища почтовых сообщений пользователя, необходимые для хранения большого объема сообщений и их архивирования.

Личные папки могут быть созданы как локально, на рабочем месте пользователя, так и на любом доступном внешнем хранилище. Личные папки используются в следующих целях:

- поддержание размера почтового ящика пользователя, располагающегося на сервере, в пределах обозначенных ему лимитов;

- организация структурированного хранилища путем создания вложенных папок;

- проведение операции архивирования почтовых сообщений, старше заданного срока отправки или получения;

- организация резервного хранилища на выделенном внешнем носителе или сервере.

- Почтовый ящик, содержащий почтовые сообщения пользователей корпоративной ЭП.

Содержимое почтовых ящиков пользователей может храниться следующими способами:

- в почтовом ящике на сервере;

- в личной папке локально на персональном пользователя;

- в архивных папках, локально на персональном пользователя;

- в общих папках, специально организованных для работы группы пользователей.

- Листы рассылок.

Список адресов доступен каждому пользователю и включает всех пользователей

- Адресная книга Пользователя – группа, созданная конкретным пользователем для структуризации своих рассылок. Такие группы недоступны для других пользователей.
- Антивирус - автоматическая система сканирования почтовых сообщений на наличие вредоносного вирусного кода (вирусов).

При обнаружении нежелательного содержания в сообщении системой антивируса вставляется сообщение с описанием причины изъятия зараженного содержания сообщения.

- Антиспам - автоматическая система сканирования почтовых сообщений на наличие нежелательной рекламной рассылки (спам).

В ЭП настроена подсистема обнаружения нежелательной почты.

Сообщения, которые определены подсистемой антиспам как нежелательные, хранятся в карантине в течение 5 дней с момента поступления, после чего безвозвратно удаляются.

3. Создание личного почтового ящика в корпоративной электронной почте образовательной организации

- Создание личного почтового ящика и его настройка для работы в корпоративной ЭП осуществляется на основании заявки руководителя структурного подразделения в информационно-техническую службу образовательной организации.
- Для каждого пользователя создается только один личный почтовый ящик.
- Для работы одним пользователем с несколькими почтовыми ящиками специалистом информационно-технической службы выполняется соответствующая настройка.
- Пользователь лично обеспечивает сохранность Личных папок на рабочем месте.

4. Обеспечение контроля почтовых ящиков

Контроль почтовых ящиков в корпоративной ЭП должен в автоматическом режиме обеспечивать выполнение следующих действий:

- направление сообщения при приближении к установленному лимиту размера личного почтового ящика;

- автоматическое блокирование возможности отправки почтовых сообщений при превышении установленных лимитов размеров личных почтовых ящиков;

- оперативное получение статистики использования и нагрузки на почтовые сервера;

- ограничение до 100 получателей в одном сообщении для всех пользователей;

- ежедневное автоматическое удаление сообщений, хранящихся более 5 дней, из папки Удаленные;

- отправление уведомлений о превышении лимита размера личного почтового ящика.

Превышение лимита размера личного почтового ящика автоматически блокируется возможность отправлять сообщения, при этом входящие сообщения продолжают приходить на личный почтовый ящик. В случае превышения лимита размера личного почтового ящика система автоматически направляет информационное сообщение о необходимости чистки личного почтового ящика. После уменьшения пользователем размера личного почтового ящика до установленного лимита (перемещением электронной почты в личную папку, общую папку или удалением), предусмотрено автоматическое восстановление заблокированных возможностей.

Каждый пользователь несет персональную ответственность за соблюдение установленного размера личного почтового ящика, а также своевременное архивирование или удаление информации.

5. Удаление личных почтовых ящиков

Удаление личных почтовых ящиков уволенных работников производится работниками инженерно-технической службы на основании данных об увольнении работника образовательного

учреждения, поступающих в информационную систему организации *(указать наименование информационной системы)*. Процедура удаления предполагает блокировку личного почтового ящика на 1 месяц и безвозвратное удаление по окончании данного срока.

Организация передачи информации, относящейся к работе, из личных почтовых ящиков увольняемых работников осуществляется руководителем соответствующего структурного подразделения на основании письменного согласия работника.

6. Ограничения использования корпоративной электронной почты

При пользовании корпоративной ЭП пользователи обязаны соблюдать следующие правила:

- соблюдать общепринятые нормы и правила обмена почтовыми сообщениями;
- строго следовать ограничениям в рассылке сведений, содержащих персональные данные и иную конфиденциальную информацию, по которым установлен особый режим доступа и использования в соответствии с законодательством Российской Федерации, локальными нормативными актами;
- перед отправлением сообщения проверять правописание, грамматику и перечитывать сообщение;
- не рассылать сообщения противозаконного или неэтичного содержания, а также содержащие угрозы в адрес других пользователей;
- запрещается осуществлять рассылку сообщений рекламного или поздравительного характера;
- неукоснительно соблюдать положения настоящего Регламента.

Информации должна рассылаться только тем адресатам, которым она действительно необходима для выполнения служебных функций.

При систематических (более 3-х раз) нарушениях пользователем настоящего Регламента, а также по обоснованной жалобе других работников образовательного учреждения на действия отправителя сообщений личный почтовый ящик такого пользователя может быть заблокирован по решению руководства на основании представления руководителя информационно-технической службы *(или иного уполномоченного лица).*

В случае необходимости руководитель информационно-технической службы *(или иное уполномоченное лицо)* направляет обоснованную служебную записку руководителю образовательного учреждения для принятия решения о наложении дисциплинарного взыскания на пользователя, допустившего нарушение.

Все пользователи в обязательном порядке знакомятся с настоящим Регламентом и Памяткой по работе с корпоративной электронной почтой образовательного учреждения, обеспечивая в работе выполнение требований указанных документов.

Приложение 12
к приказу от 29.08.2022 № 263

Памятка
по работе с корпоративной электронной почтой МАОУ «ООШ№280»

Политика использования электронной почты является важнейшим элементом корпоративной политики информационной безопасности МАОУ «ООШ № 280».

Корпоративная электронная почта может быть использована только в служебных целях. Использование электронной почты в других целях категорически запрещено.

Содержимое электронного почтового ящика сотрудника может быть проверено без предварительного уведомления по требованию непосредственного либо вышестоящего руководителя.

При работе с корпоративной системой электронной почты сотрудникам образовательной организации запрещается:

- распространять информацию ограниченного доступа, предназначенную для служебного использования, в том числе сведения, составляющие персональные данные и иную конфиденциальную информацию;
- распространять материалы, защищаемые авторскими правами;
- использовать адрес корпоративной почты для оформления подписок;
- публиковать свой адрес либо адреса других сотрудников на общедоступных Интернет-ресурсах (форумы, конференции и т.п.) за исключением случаев служебной необходимости;
- осуществлять массовую рассылку почтовых сообщений рекламного характера;
- рассылать через электронную почту материалы, содержащие вирусы и другие вредоносные продукты и программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ для осуществления несанкционированного доступа;
- распространять угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, запрещённую российским законодательством;
- предоставлять иным лицам пароль доступа к своему почтовому ящику.

Приложение 13
к приказу от29.08.2022 № 263

Регламент доступа и использования ресурсов сети Интернет в образовательной организации

1. Общие положения

1.1. Положение предназначено для сотрудников образовательной организации, выполнение должностных обязанностей которых связано с использованием персональных компьютеров, и обучающихся и определяет их полномочия, обязанности и ответственность при использовании информационных ресурсов глобальной компьютерной сети Интернет.

1.2. Положение является обязательным для выполнения всеми сотрудниками образовательной организации - пользователями персональных компьютеров в части, касающейся их.

1.3. В Положении используются следующие сокращения и основные понятия:

- ПК - персональный компьютер;
- ИС - информационная сеть;
- пользователь – сотрудник образовательной организации, выполнение должностных обязанностей которого связано с использованием ПК в ИС образовательной организации, и обучающийся;
- ИР - информационные ресурсы (отдельные документы и отдельные массивы документов, базы данных, другие виды информационного обеспечения в ИС с использованием ПК);
- ИТ-служба – информационно-техническая служба;
- администратор – сотрудник ИТ-службы, ответственный за подключение к глобальной сети Интернет и обеспечение работоспособности, надежности сети, сохранности и защиты информационных ресурсов;
- трафик - объем информации, полученной пользователем из глобальной компьютерной сети Интернет;
- развлекательные сайты - сайты знакомств, игровые сайты, а также любые сайты, которые не относятся к направлению деятельности сотрудника.
- chat – ресурс Интернет, предоставляющий возможность пользователям осуществлять переписку в реальном времени.
- skype – ресурс Интернет, предоставляющий возможность пользователям осуществлять голосовое и видео общение в реальном времени.

1.4. Руководители структурных подразделений, пользователи и администраторы обязаны знать и выполнять нормативные правовые акты, затрагивающие вопросы защиты информации, в том числе персональных данных, и информационной безопасности в части соблюдения требований и ограничений по использованию ИР.

1.5. Руководители структурных подразделений в обязательном порядке организуют ознакомление пользователей с нормативными правовыми актами, указанными в настоящем Регламенте.

1.6. Доступ к сети Интернет осуществляется с рабочего ПК пользователя. Ответственность за действия на компьютере другого человека несет пользователь ПК, с которого совершено это действие.

1.7. Работа пользователей в сети Интернет отслеживается с помощью специального программного обеспечения. На основе регистрации журнала работы проводится анализ по следующим параметрам:

- перечень используемых пользователем ресурсов;

- объем использованного трафика и его стоимость по тарифам провайдера.

1.8. Настоящее Положение может уточняться и дополняться в установленном порядке.

2. Требования к Пользователю

2.1. Данный раздел отражает полномочия, обязанности и ограничения прав пользователей глобальной компьютерной сети Интернет.

2.2. Пользователь имеет право оспаривать решение администратора через своего непосредственного руководителя, который, в свою очередь, обращается в ИТ-службу. Если обе стороны не могут прийти к консенсусу, тогда вопрос рассматривает руководитель образовательной организации или уполномоченное им лицо.

2.3 **Пользователь обязан:**

- знать и уметь пользоваться антивирусным программным обеспечением. При обнаружении вируса он должен сообщить об этом администратору и не производить никаких действий с информацией, зараженной вирусом;
- информировать администратора о любых нарушениях, которые могут привести к несанкционированному доступу, модификации, разрушению, удалению информационных ресурсов или сбоям в работе сети.

2.4. **Пользователю запрещается**:

- загружать из сети, самостоятельно устанавливать прикладное, операционное, сетевое и другие виды программного обеспечения, а также осуществлять обновления, если эта работа не входит в его должностные обязанности;
- использовать ресурсы сети Интернет в не служебных целях;
- допускать к работе в сети Интернет со своего ПК посторонних лиц;
- подключаться к ресурсам сети Интернет, используя свой ПК через не служебный канал доступа (сотовый телефон, модем и др. устройства).

3. Требования к администратору

3.1. Данный раздел отражает функциональные обязанности и полномочия администратора, обеспечивающего доступ к сети Интернет.

3.2. **Администратор обязан**:

- производить подключение к сети Интернет только через сетевой экран (Firewall) для обеспечения защиты информационной сети;
- знать и правильно использовать аппаратно - программные средства защиты информации и обеспечивать сохранность информационных ресурсов с помощью этих средств;
- оказывать методическую и консультационную помощь пользователям по вопросам, входящим в его компетенцию;
- ежемесячно вести учет и анализ использования ресурсов сети Интернет по каждому пользователю, предоставлять этот отчет руководству организации;
- информировать руководителей структурных подразделений о любых нарушениях требований настоящего Положения и других негативных ситуациях, которые могут привести к несанкционированному доступу, модификации, разрушению, удалению информационных ресурсов или сбоям в работе сети;

3.3. **Администратор имеет право:**

- при обнаружении факта доступа пользователя к развлекательным сайтам, Chat или Skype запретить доступ к соответствующему ресурсу;

- при обнаружении использования пользователем программных продуктов, которые могут привести к несанкционированному доступу, модификации, разрушению, удалению информационных ресурсов или сбоям в работе сети, запретить доступ к сети Интернет.

4. Порядок предоставления доступа пользователям к сети Интернет

4.1. Система контроля Интернет-доступа в организации предусматривает следующие автоматические ограничения:

- запрет входа на определенные сайты;
- запрет определенных Интернет-протоколов;
- антивирусную проверку Интернет-трафика, с автоматическим блокированием зараженного или подозрительного содержимого;
- запрет скачивания определенных типов файлов;
- автоматическое отключение пользователя и/или групп пользователей от платных ресурсов, по достижении ими ежедневного, еженедельного или ежемесячного лимита.

4.2. Система контроля Интернет-доступа осуществляет сбор статистики использования Интернета пользователями. Настоящая статистика доступна руководству организации, системному администратору и может служить причиной ограничения или изменения прав доступа пользователей к сети Интернет.

4.3. Определяются следующие возможные ограничения доступа к Интернету для пользователей:

- доступ в Интернет – доступ к сети Интернет с рабочего места;
- ограничения (внешняя электронная почта) – доступ к сайтам, предоставляющим услуги электронной почты (mail.ru, mail.yandex.ru, mail.e1.ru и др.);
- ограничения (интернет-пейджеры) – доступ к icq, mail.ru-агенту и др. интернет-пейджерам;
- ограничения (порнография, развлечения, баннеры) – ограничения в соответствии со списком запрещенных сайтов официального **Реестра запрещенных сайтов, единого реестра Роскомнадзора;**
- ограничения (социальные сети) – ограничения по спискам соответствующих сайтов (odnoklassniki.ru, vkontakte.ru и т.д.);
- ограничения (поиск работы) – сайты объявлений о вакансиях и резюме;
- ограничения на стоимость использованного в день трафика.

4.4. Доступ к сети Интернет пользователям предоставляется, исходя из служебной необходимости, после определения необходимых ограничений доступа (см. пункт 4.3 регламента) на основании служебной записки на имя руководителя организации от руководителя структурного подразделения, согласованной руководителем образовательной организации.

4.5. Изменение прав доступа и различных ограничений, а также ручное включение пользователя после автоматического отключения (после превышения дневного лимита) производиться также после служебной записки (или объяснительной) на имя системного администратора от руководителя подразделения, согласованной руководителем образовательной организации.

4.6. В случае возникновения претензий или вопросов, касающихся конкретного запрещенного сайта, типа файла, невозможности продолжения работы в сети Интернет пользователь обращается к администратору через своего непосредственного руководителя. Если

этим лицам не удается разрешить возникшую проблему, вопрос рассматривает руководитель образовательной организации или иное уполномоченное им лицо.

Приложение 14
к приказу от 29.08.2022 № 263

ПОРЯДОК
учета и использования машинных носителей информации, содержащих персональные данные и иную конфиденциальную информацию

1. Общие положения

Настоящий Порядок разработан в соответствии с Федеральным законом № 149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 г. N 152-ФЗ «О персональных данных», ГОСТ Р ИСО/МЭК 17799-2005 «Практические правила управления информационной безопасностью» и другими нормативными правовыми актами, и устанавливает порядок учета и использования машинных носителей информации для обработки персональных данных.

2. Основные термины, сокращения и определения

Администратор информационной системы – технический специалист, обеспечивает ввод в эксплуатацию, поддержку и последующий вывод из эксплуатации программного обеспечения (ПО) и оборудования вычислительной техники.

АРМ – автоматизированное рабочее место пользователя (персональный компьютер (ПК) с прикладным ПО) для выполнения определенной производственной задачи.

ИБ – информационная безопасность – комплекс организационно-технических мероприятий, обеспечивающих конфиденциальность, целостность и доступность информации.

ИС – информационная система – система, обеспечивающая хранение, обработку, преобразование и передачу информации с использованием компьютерной и другой техники.

Машинный носитель информации – материальный носитель, используемый для хранения и передачи электронной информации.

ПК – персональный компьютер.

ПО – программное обеспечение вычислительной техники.

ПО вредоносное – ПО или изменения в ПО, приводящие к нарушению конфиденциальности, целостности и доступности критичной информации.

Пользователь – работник Оператора, использующий ПК и носители информации для выполнения своих служебных обязанностей.

3. Порядок использования машинных носителей информации

3.1. Под использованием машинных носителей информации в ИС понимается их подключение к инфраструктуре ИС с целью обработки, приема/передачи информации между ИС и носителями информации.

3.2. В ИС допускается использование только учтенных машинных носителей информации, которые являются собственностью Оператора и подвергаются регулярной ревизии и контролю.

3.3. К машинным носителям конфиденциальной информации предъявляются те же требования ИБ, что и для стационарных АРМ (целесообразность дополнительных мер обеспечения ИБ определяется администраторами ИС).

3.4. Машинные носители конфиденциальной информации предоставляются по инициативе Руководителей структурных подразделений в случаях:

- необходимости выполнения вновь принятым Пользователем своих должностных обязанностей;
- возникновения у Пользователя производственной необходимости.

4. Порядок учета, хранения и обращения со съемными машинными носителями конфиденциальной информации (персональных данных)

4.1. Все находящиеся на хранении и в обращении съемные машинные носители с конфиденциальной информацией (персональными данными) подлежат учёту.

4.2. Каждый съемный машинный носитель с записанной на нем конфиденциальной информацией (персональными данными) должен иметь этикетку, на которой указывается его уникальный учетный номер.

4.3. Учет и выдачу съемных машинных носителей конфиденциальной информации (персональных данных) осуществляют уполномоченные сотрудники структурных подразделений, на которых возложены функции хранения машинных носителей персональных данных. Факт выдачи съемного машинного носителя исполнителю фиксируется в журнале учета съемных машинных носителей конфиденциальной информации.

4.4. Пользователи получают учтенный съемный носитель от уполномоченного сотрудника для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнале учета. По окончании работ Пользователь сдает съемный носитель для хранения уполномоченному сотруднику, о чем делается соответствующая запись в журнале учета.

4.5. При использовании Пользователями машинных носителей с конфиденциальной информацией (персональными данными) необходимо:

- соблюдать требования настоящего Порядка;
- использовать машинные носители информации исключительно для выполнения своих служебных обязанностей;
- ставить в известность администраторов ИС о любых фактах нарушения требований настоящего Порядка;
- бережно относится к машинным носителям конфиденциальной информации (персональных данных);
- обеспечивать физическую безопасность машинных носителей информации всеми разумными способами;
- извещать администраторов ИС о фактах утраты (кражи) машинных носителей конфиденциальной информации (персональных данных).

4.6. При использовании машинных носителей конфиденциальной информации (персональных данных) запрещается:

- использовать носители конфиденциальной информации (персональных данных) в личных целях;
- передавать носители конфиденциальной информации (персональных данных) другим лицам (за исключением администраторов ИС);
- хранить съемные носители с конфиденциальной информацией (персональными данными) вместе с общедоступными данными, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;
- выносить съёмные носители с конфиденциальной информацией (персональными данными) из служебных помещений для работы с ними на дому и т. д.

4.7. Любое взаимодействие (обработка, прием/передача информации), инициированное сотрудником между ИС и неучтенными (личными) носителями информации, рассматривается как несанкционированное (за исключением случаев согласованных с администраторами ИС заранее). Администратор ИС оставляет за собой право блокировать или ограничивать использование машинных носителей информации.

4.8. В случае выявления фактов несанкционированного и/или нецелевого использования машинных носителей конфиденциальной информации (персональных данных) инициализируется служебная проверка, проводимая комиссией, состав и полномочия которой определяется приказом Оператора. По факту выясненных обстоятельств составляется акт расследования инцидента и передается руководителю структурного подразделения для принятия мер согласно локальным нормативным актам Оператора и действующему законодательству.

4.9. Информация, хранящаяся на машинных носителях конфиденциальной информации (персональных данных), подлежит обязательной проверке на отсутствие вредоносного ПО.

4.10. При отправке или передаче конфиденциальной информации (персональных данных) адресатам на съемные машинные носители записываются только предназначенные адресатам данные. Отправка конфиденциальной информации (персональных данных) адресатам на съемных машинных носителях осуществляется в порядке, установленном для документов для служебного пользования.

4.11. Вынос съемных машинных носителей конфиденциальной информации (персональных данных) для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя структурного подразделения.

4.12. В случае утраты или уничтожения съемных машинных носителей конфиденциальной информации (персональных данных) либо разглашении содержащихся в них сведений немедленно ставится в известность руководитель соответствующего структурного подразделения. На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы учета съемных носителей конфиденциальной информации (персональных данных).

4.13. Съемные носители конфиденциальной информации (персональных данных), пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению в соответствии с «Порядком уничтожения документов и машинных носителей информации, содержащих персональные данные».

4.14. В случае увольнения или перевода работника в другое структурное подразделение, предоставленные ему машинные носители конфиденциальной информации (персональных данных) изымаются уполномоченным сотрудником структурных подразделений, на которого возложены функции хранения машинных носителей персональных данных.

5. Ответственность

Пользователи и администраторы информационной системы, нарушившие требования настоящего Положения, несут ответственность в соответствии с действующим законодательством и локальными нормативными актами Оператора.

Приложение 15
к приказу от29.08.2022 № 263

Требования
к оборудованию помещений и размещению технических средств, используемых для обработки персональных данных

- Настоящие Требования определяют порядок оборудования выделенных помещений и условия размещения в них технических средств (персональных компьютеров, серверов и т.п.), используемых для обработки персональных данных в МАОУ «ООШ № 280».
- Расположение выделенных помещений и размещаемых в них технических средств должно исключать возможность бесконтрольного проникновения в эти зоны посторонних лиц и гарантировать сохранность находящихся в них конфиденциальных документов, содержащих персональные данные.
- Размещение оборудования и технических средств, предназначенных для обработки персональных данных, должно соответствовать требованиям техники безопасности, санитарным нормам, а также требованиям пожарной безопасности.
- Внутренняя планировка и расположение рабочих мест в выделенных помещениях должны обеспечивать исполнителям сохранность доверенных им конфиденциальных документов и сведений, содержащих персональные данные.
- Входные двери выделенных помещений должны быть оборудованы замками, гарантирующими санкционированный доступ в них в нерабочее время.
- В выделенные помещения по утвержденному списку допускаются руководство организации, сотрудники службы (*ответственный за*) информационной безопасности, сотрудники информационно-технической службы, иные уполномоченные лица и исполнители, имеющие прямое отношение к приему, обработке и передаче персональных данных.
- Допуск в выделенные помещения вспомогательного и обслуживающего персонала (уборщицы, электромонтеры, сантехники и т.д.) производится только при служебной необходимости и в сопровождении ответственного за помещение, при этом необходимо принять меры, исключающие визуальный просмотр конфиденциальных документов, содержащих персональные данные.
- По окончании рабочего дня выделенные помещения необходимо закрывать .
- Сдачу ключей и выделенных помещений под охрану, а также получение ключей и вскрытие выделенных помещений имеют право производить только сотрудники, работающие в этих помещениях и внесенные в утвержденный руководством организации список с образцами подписей этих сотрудников. Список хранится у ответственного дежурного подразделения безопасности.
- Перед вскрытием выделенных помещений должна быть проверена целостность и исправность замков. При обнаружении повреждения замков или других признаков, указывающих на возможное проникновение в эти помещения посторонних лиц, помещение не вскрывается, а о случившемся немедленно информируется руководство организации (или иное уполномоченное лицо).
- В случае утраты ключа от входной двери выделенного помещения немедленно ставится в известность руководитель организации (или иное уполномоченное лицо).
- В выделенных помещениях, где установлены средства защиты информации от утечки по техническим каналам, запрещается приносить и использовать радиотелефоны/сотовые телефоны и другую радиоаппаратуру.
- На случай пожара, аварии или стихийного бедствия должны быть разработаны специальные инструкции, утвержденные руководством организации, в которых предусматривается вызов администрации, должностных лиц, вскрытие выделенных помещений, очередность и порядок спасения конфиденциальных документов, содержащих персональные данные, и дальнейшего их хранения.

Приложение 16
к приказу от29.08.2022 № 263

ПОРЯДОК
уничтожения, блокирования персональных данных

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 *(напр. руководитель службы информационной безопасности)* 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 *(напр. руководитель службы информационной безопасности)* 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 *(напр. руководитель службы информационной безопасности)* 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 *(напр. руководитель службы информационной безопасности)* 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 *(напр. руководитель службы информационной безопасности)* 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).	В 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, 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“ 1.4Mb (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 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

4.2. 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 носитель.

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.

Приложение 17
к приказу от 29.08.2022 № 263

УТВЕРЖДАЮ

_____
(Ф.И.О., подпись)

«____» _____ 20___ г.

А К Т №

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

_____ «____»_____ 20___ г
(место уничтожения) (дата уничтожения)

Комиссия, в составе:
Председатель: _____,
(должность, фамилия, имя, отчество)
Члены:
_____
(должность, фамилия, имя, отчество)
_____
(должность, фамилия, имя, отчество)

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:

_____ _____
(подпись) (Ф. И. О.)

_____ _____
(подпись) (Ф. И. О.)

_____ _____
(подпись) (Ф. И. О.)

Приложение 18
к приказу от29.08.2022 № 263

А К Т №

акта выявления нарушений в сфере защиты персональных данных и иной конфиденциальной информации

_____ «____ »_____ 20___ г

Настоящий акт составлен в том, что в

_____

(наименование структурного подразделения, где выявлено нарушение)

ФИО и должность лица, допустившего нарушение_____

допущено нарушение установленных требований в сфере защиты персональных данных и иной конфиденциальной информации.

Содержание нарушения_____

_____

Требования каких нормативных документов нарушены_____

_____

_____

_____

_____

Комиссия (или уполномоченное лицо), выявившая нарушения

Подписи

_____ _____

(подпись) (Ф. И. О.)

_____ _____

(подпись) (Ф. И. О.)

_____ _____

(подпись) (Ф. И. О.)

С актом ознакомлены:

подпись лица, допустившего нарушение_____(ФИО_____)

подпись руководителя структурного подразделения, где допущено нарушение_____(ФИО_____)

Приложение 19
к приказу от 29.08.2022 № 263

Форма

Начат «___» _____ 20__ г.

Окончен «___» _____ 20__ г.

На _____ листах

ЖУРНАЛ
журнала регистрации выявленных нарушений в сфере защиты персональных данных и иной конфиденциальной информации

№	Дата выявления нарушения	Подразделение, где выявлено нарушение и допустившее нарушение лицо (ФИО, должность)	Кем и при каких обстоятельствах выявлено нарушение (жалоба, плановая проверка и т.д.)	Содержание нарушения	Требования, каких нормативных документов нарушены
1	2	3	4	5	6

Корректирующие и предупреждающие действия по устранению нарушения и предотвращению нарушения в дальнейшем	Ответственное за устранение лицо выявленного нарушения лицо (ФИО, должность и его подпись)	Срок устранения нарушения	Отметка о контроле за выполнением (дата, ФИО и должность проверяющего)
7	8	9	10

Приложение 20
к приказу от 29.08.2022 № 263

Положение о службе информационной безопасности МАОУ «ООШ№280»

1. Общие положения

Служба информационной безопасности (далее Служба) образовательной организации (далее Оператор) создаётся в целях выполнения требований действующего законодательства Российской Федерации, иных нормативно-правовых актов, регламентирующих обеспечение защиты информации, в том числе обеспечение безопасности при обработке персональных данных, а также обеспечение защиты и безопасности информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных.

2. Структура

Структура и штатная численность Службы определяются приказом руководителя Оператора. Служба создаётся на функциональной основе, т.е. без выделения штатных единиц, и включает заместителя руководителя учреждения, в ведении которого находится подразделение по информационным технологиям, руководителя (или специалиста) подразделения по информационным технологиям, руководителей (при их отсутствии специалистов) кадрового и юридического подразделений, (кто конкретно указывается в соответствующем приказе руководителя). Руководство Службой по приказу руководителя возлагается на заместителя руководителя, в ведении которого находится подразделение по информационным технологиям.

3. Задачи

Основные задачи Службы заключаются в следующем.

1. Разработка и реализация комплекса организационных и технических мер, направленных на выполнение установленных требований к обеспечению безопасности и защите информации, в том числе персональных данных.
2. Обеспечение постоянного контроля в подразделениях Оператора за выполнением установленных требований к обеспечению безопасности и защите информации, в том числе персональных данных.
3. Разработка и внесение предложений руководству Оператора по совершенствованию и развитию корпоративной системы обеспечения безопасности и защиты информации, в том числе персональных данных.

4. Функции

Для выполнения поставленных задач Служба осуществляет следующие функции.

1. Готовит и представляет на рассмотрение руководству Оператора проекты локальных нормативных актов по вопросам обеспечения защиты информации, в том числе персональных данных.
2. Организует и проводит во взаимодействии с заинтересованными подразделениями классификацию информационных систем на этапе создания информационных систем или в ходе их эксплуатации (для ранее введенных в эксплуатацию и (или) модернизируемых информационных систем) с целью установления методов и способов защиты информации, необходимых для обеспечения безопасности персональных данных в соответствии с установленными требованиями.

3. Разрабатывает и реализует комплекс организационных и мер по обеспечению защиты информации от:

- неправомерного доступа;
- уничтожения;
- модифицирования;
- блокирования;
- копирования;
- предоставления;
- распространения;
- а также от иных неправомерных действий в отношении такой информации.

4. Для защиты информации, в том числе персональных данных от неправомерного доступа Служба обеспечивает:

- контроль за строгим соблюдением принятого Оператором Порядка доступа к конфиденциальной информации, в том числе к персональным данным;
- предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
- своевременное обнаружение фактов несанкционированного доступа к информации;
- предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
- возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней.

5. Служба при создании и эксплуатации корпоративных информационных систем:

- самостоятельно разрабатывает и внедряет методы и способы защиты информации, соответствующие установленным требованиям;
- согласовывает исполнителю планируемые для использования в целях защиты информации методы и способы при условии их соответствия установленным требованиям.

6. Служба:

- разрабатывает и реализует меры организационного и технического по недопущению воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
- организует и (или) проводит экспертизу технических средств, используемых при обработке информации на предмет соответствия возможностей защиты информации указанных средств установленным требованиям.

7. Служба разрабатывает и реализует меры по информированию и обучению персонала Оператора, в том числе вновь принимаемых на работу лиц, по вопросам защиты информации и персональных данных.

8. Служба контролирует выполнение установленных требований по:

- осуществлению обмена персональными данными при их обработке в информационных системах по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения технических средств:
- размещению информационных систем, специального оборудования и охране помещений, в которых ведется работа с персональными данными, организации режима обеспечения безопасности в этих помещениях в части обеспечения сохранности носителей персональных данных и средств защиты информации, а также исключения возможности неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц;
- соблюдению парольной защиты;
- соблюдению установленного регламента работы с электронной почтой;

- соблюдению требований к программному обеспечению и его использованию.

9. В соответствии с установленными нормативно-правовыми актами требованиями Служба обеспечивает:

- определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

- разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

- проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

- установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

- обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

- учет лиц, допущенных к работе с персональными данными в информационной системе;

- контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

- разбор и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

- описание системы защиты информации, в том числе персональных данных;

- ежегодное планирование работы по совершенствованию системы защиты информации, в том числе персональных данных;

- подготовку и предоставление отчётов руководству Оператора, а также по требованию надзорных и иных уполномоченных органов об организационных и технических мероприятиях по защите информации, в том числе персональных данных;

- постоянный контроль за обеспечением уровня защищенности информации.

5. Взаимодействие

Для решения поставленных задач и осуществления предусмотренных настоящим Положением функций Служба взаимодействует:

- с руководителем Оператора и его заместителями;

- с любыми иными подразделениями Оператора;

- с государственными, муниципальными органами, учреждениями и организациями, с надзорными органами, а также с иными органами, предприятиями и организациями.

В ходе взаимодействия руководитель и сотрудники Службы:

- в установленном порядке, получают необходимую для осуществления деятельности Службы информацию, разъяснения, уточнения, нормативные и иные документы;

- готовит и в установленном порядке вносят руководству Оператора предложения по проведению организационных и технических мероприятий, изданию локальных нормативных актов, принятию иных мер по установленным направлениям деятельности в сфере защиты информации, в том числе персональных данных;

- готовят и в установленном порядке предоставляют информацию по находящимся в их компетенции вопросам в сфере защиты информации, в том числе персональных данных, по запросам подразделений Оператора, государственных, муниципальных органов, учреждений и организаций, надзорных органов, а также иных органов, предприятий и организаций.

6. Ответственность

Руководитель Службы несет ответственность перед руководством Оператора согласно действующему законодательству, нормативно-правовым и локальным нормативным правовым актам за обеспечение:

- выполнения поставленных перед подразделением задач и функций,
- работы с документами и их сохранности, своевременного и качественного исполнения поручений и обращений,
- выполнения требований правил внутреннего трудового распорядка,
- соблюдения в подразделении правил противопожарной безопасности.

Материальную ответственность за сохранность имущества Оператора несут сотрудники Службы, принявшие его на ответственное хранение, согласно действующему законодательству, локальным нормативным правовым актами и договором о материальной ответственности.

Ответственность перед руководителем подразделения за оперативную работу с поступающими документами и контроль за их исполнением в подразделении, несет сотрудник подразделения, назначенный руководителем Оператора.

Все сотрудники Службы несут ответственность перед руководителем Службы и руководством Оператора за своевременное и качественное выполнение:

- требований выполнения действующего законодательства Российской Федерации, иных нормативно-правовых документов, регламентирующих обеспечение защиты информации, в том числе обеспечение безопасности при обработке персональных данных;
- обязанностей, предусмотренных Трудовым кодексом РФ, правилами внутреннего трудового распорядка, коллективным договором, настоящим Положением, трудовыми договорами и должностными инструкциями.

Приложение 21
к приказу от 29.08.2022 № 263

Форма

Начат «___» _____ 20__ г.

Окончен «___» _____ 20__ г.

На _____ листах

ЖУРНАЛ
регистрации используемого программного обеспечения (ПО)

№	Наименование лицензионного ПО	Количество лицензий	Наименование структурного подразделения	ФИО пользователя, должность	Назначенные права по использованию ПО	Дата предоставления ПО	ФИО и подпись системного администратора

Приложение 22
к приказу от 29.08.2022 № 263

Форма

Начат «___» _____ 20__ г.

Окончен «___» _____ 20__ г.

На _____ листах

ЖУРНАЛ
учета носителей, содержащих персональные данные и иную конфиденциальную информацию

Учетный номер	Дата постановки на учет	Вид машинного носителя, место его хранения (размещения)	Ответственный за использование и хранение		
			Ф.И.О.	подпись	Дата получения
1	2	3	4	5	6

Дата и номер акта уничтожения персональных данных и иной конфиденциальной информации	Дата и номер акта уничтожения машинного носителя, содержащего персональные данные и иную конфиденциальную информацию
7	8