Приложение № 1.
к приказу № 94 от 30.08.2022
от _____ №_____

Инструкция
по работе пользователей информационной системы персональных данных МОУ Ахматовская ООШ

Общие положения.

1.1 Настоящая инструкция определяет задачи, функции, обязанности, права и ответственность пользователей информационной системы персональных данных (далее – ИСПДн) **МОУ Ахматовская ООШ** (далее – Учреждение).

1.2 Пользователями ИСПДн являются сотрудники Учреждения, допущенные к работе в ИСПДн.

1.3 Доведение Инструкции до сотрудников Учреждения в части их касающейся осуществляется администратором безопасности информации ИСПДн под роспись в Листе ознакомления с данной инструкцией.

2. Обязанности пользователя.

При эксплуатации ИСПДн пользователь **обязан**:

2.1 Руководствоваться требованиями следующих документов:

– настоящая инструкция;

– «Инструкция по проведению антивирусного контроля в ИСПДн», в части их касающейся;

– «Инструкция по применению парольной защиты и личных идентификаторов в ИСПДн», в части их касающейся;

– «Инструкция об организации учета, хранения и выдачи машинных носителей, содержащих персональные данные ИСПДн», в части их касающейся».

2.2 Помнить личные пароли и идентификаторы.

2.3 Соблюдать установленную технологию обработки информации.

2.4 Руководствоваться при работе в ИСПДн требованиям эксплуатационной документацией на технические средства и средства защиты информации, применяемые в ИСПДн.

2.5 Размещать устройства вывода информации технических средств ИСПДн таким образом, чтобы была исключена возможность просмотра посторонними лицами информации, содержащей персональные данные.

2.6 При выходе в течение рабочего дня из контролируемой зоны помещений, в котором размещается ИСПДн, пользователь обязан блокировать ввод-вывод информации на своем рабочем месте ИСПДн.

При эксплуатации ИСПДн пользователю **запрещается**:

– подключать к средствам вычислительной техники (далее – СВТ) нештатные устройства;

– производить загрузку нештатной операционной системы с внешнего носителя;

– самостоятельно вносить изменения в состав, конфигурацию и размещение ИСПДн;

– самостоятельно вносить изменения в состав, конфигурацию и настройку программного обеспечения (ПО), установленного в ИСПДн;

– устанавливать запрещенное к использованию ПО (средства обработки и отладки);

– самостоятельно вносить изменения в размещение, состав и настройку средств защиты информации (далее – СЗИ) ИСПДн;

– сообщать устно, письменно или иным способом другим лицам пароли, передавать личные идентификаторы, ключевые носители и другие реквизиты доступа к ресурсам ИСПДн.

3. Права пользователя.

Пользователь ИСПДн имеет право:

– обращаться к администратору безопасности информации ИСПДн с просьбой об оказании технической и методической помощи по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн, по использованию установленных программных и технических средств ИСПДн, а также по вопросам эксплуатации установленных СЗИ;

– обращаться к ответственному за обеспечение безопасности персональных данных в ИСПДн по вопросам эксплуатации ИСПДн (выполнение установленной технологии обработки информации, инструкций и других документов по обеспечению информационной безопасности объекта и защиты персональных данных);

– обращаться к ответственному за обеспечение безопасности персональных данных в ИСПДн по вопросам выполнения режимных мер при обработке персональных данных.

4. Ответственность пользователя.

Пользователь несет персональную ответственность:
за соблюдение установленной технологии обработки персональных данных;

– за соблюдение режима конфиденциальности при обработке и хранении в ИСПДн персональных данных;

– за правильность понимания и полноту выполнения задач, функций, прав и обязанностей, возложенных на него при работе в ИСПДн;

– за соблюдение требований нормативных правовых актов, приказов, распоряжений и указаний, определяющих порядок организации работ по информационной безопасности при работе с персональными данными.

Приложение № 2
к приказу 44/2 - ОД
от 06. 08 2018 №

Правила
обработки персональных данных в информационной системе персональных данных МОУ Ахматовская ООШ

1. **Общие положения.**

1.1. Настоящие Правила обработки персональных данных (далее — Правила) в информационной системе персональных данных (далее – ИСПДн)**МОУ Ахматовская ООШ** (далее – Учреждение) разработаны в соответствии с законодательством Российской Федерации и законодательством Тверской области и устанавливают процедуры, направленные на соблюдение законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований.

2. **Процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных.**

2.1. Источником информации о нарушениях законодательства Российской Федерации в сфере персональных данных могут служить:

– сообщения субъекта персональных данных;

– уведомления/сообщения органов, осуществляющих контроль или надзор за деятельностью Учреждения в сфере защиты прав субъектов персональных данных.

2.2. При получении сообщения о нарушениях законодательства Российской Федерации в сфере персональных данных по электронной почте или по телефонному звонку необходимо убедиться в достоверности полученной информации (например, путем совершения «обратного» звонка по указанным в сообщении телефонам, проверки данных указанных в подписи сообщения или названных при звонке).

2.3. Работник Учреждения, получивший информацию о нарушениях законодательства Российской Федерации в сфере персональных данных, сообщает об этом должностному лицу Учреждения, ответственному за организацию обработки персональных данных работников (далее – Ответственному).

2.4. Ответственный в письменной форме сообщает о факте нарушения директору Учреждения.

2.5. Приказом директора Учреждения, для разбора факта нарушения законодательства Российской Федерации в сфере персональных данных работников учреждения создается комиссия, в состав которой могут входить:

– Ответственный за организацию обработки персональных данных;

– начальник отдела, в котором зафиксирован факт нарушения законодательства Российской Федерации в сфере персональных данных;

– работник Учреждения, права которого в сфере персональных данных нарушены.

2.6. Комиссия собирает и анализирует все данные об обстоятельствах нарушения законодательства Российской Федерации в сфере персональных данных (электронные письма, файлы протоколов информационных систем, показания сотрудников и др.), устанавливает, имела ли место утечка сведений и обстоятельства ей сопутствующие, определяет перечень лиц, виновных в нарушении предписанных федеральным законодательством мероприятий по защите персональных данных, устанавливает причины и условия, способствовавшие нарушению.

2.7. По итогам работы комиссии директору Учреждения предоставляется отчет, в котором указываются причина нарушения законодательства Российской Федерации в сфере персональных данных, последствия данного факта, лица, виновные в возникновении нарушения законодательства Российской Федерации в сфере персональных данных, предложения о наказании виновных лиц и мерах по недопущению подобных инцидентов в будущем.

3. Процедуры, определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения.

3.1. Процедуры, определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории работников, персональные данные которых обрабатываются, сроки их обработки и хранения сведены в таблицу.

№ п/п	Цели обработки персональных данных	Содержание обрабатываемых персональных данных	Категории субъектов персональных данных	Сроки обработки/ хранения персональных данных
1.	Учет обучающиеся в Учреждении	фамилия, имя, отчество, дата рождения, пол, возраст, место рождения, серия и номер основного документа удостоверяющего личность, сведения о дате выдачи указанного документа и выдавшем его органе, адрес места жительства, почтовый адрес, телефон, Email, номер страхового свидетельства государственного пенсионного страхования (СНИЛС), гражданство, состав семьи, социальное положение, физическая группа ребенка, группа здоровья, сведения о девиантном поведении ребенка, группа инвалидности, категория инвалидности, иные сведения, необходимые для определения отношений обучения и воспитания	учащихся Учреждения, их законных представители	достижении целей обработки или при наступлении иных законных оснований

4. Порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований.

4.1. По окончании указанных в разделе 3 сроков хранения персональных данных, они физически уничтожаются с целью невозможности восстановления и дальнейшего использования.

Уничтожение персональных данных на программно-технических средствах ИСПДн производится специальными программными средствами, осуществляющими удаление информации без возможности ее восстановления.

4.2. Для уничтожения персональных данных приказом директора Учреждения, создается комиссия, состав которой могут входить:

– Ответственный;

– начальник отдела Учреждения, в котором проводится обработка персональных данных;

– работник Учреждения, имеющий право обработки персональных данных работников Учреждения.

Уничтожение производится в присутствии всех членов комиссии, которые несут персональную ответственность за правильность и полноту уничтожения персональных данных.

4.3. По результатам работы комиссии составляется акт в трех экземплярах уничтожения персональных данных работников Учреждения на программно-технических средствах ИСПДн (Приложение к Правилам).

Приложение № 4
к приказу
№ 44/2-ОД
от 06.09.2018. №

Порядок доступа работников
МОУ Ахматовская ООШ

1. Настоящий порядок разработан в соответствии с законодательством Российской Федерации и законодательством Тверской области и определяет порядок доступа в помещения **МОУ Ахматовская ООШ** (далее – Учреждение), где обрабатываются персональные данные в рамках информационной системы персональных данных (далее – ИСПДн).

2. Перечень сотрудников Учреждения, допущенных к работе с персональными данными в ИСПДн определяется приказом директора Учреждения.

3. В своей работе должностные лица, допущенные к обработке персональных данных в ИСПДн, должны руководствоваться требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», правовых документов Правительства Российской Федерации, ФСТЭК России, ФСБ России, а также настоящим порядком.

4. Ответственность за обеспечение безопасности персональных данных и надлежащего режима доступа к ИСПДн возлагается на директора Учреждения.

5. Помещения, в которых обрабатываются персональные данные в рамках ИСПДн, должны быть защищены от физического проникновения посторонних лиц. Доступ лиц, не причастных к непосредственной обработке персональных данных, в эти помещения должен быть исключен.

6. Системы обработки и хранения персональных данных в ИСПДн должны быть расположены так, чтобы исключить возможность случайного или преднамеренного доступа к ним неуполномоченных лиц в процессе их обработки.

7. Пользователи ИСПДн обязаны:

– пройти инструктаж о соблюдении требований к защите персональных данных;

– строго следить за соблюдением режима разграничения доступа, незамедлительно информировать непосредственного руководителя и заместителя директора Учреждения, ответственного за организацию обработки персональных данных, о всех случаях утечки или разрушения обрабатываемой в ИСПДн защищаемой информации;

– перед началом обработки в ИСПДн персональных данных работников Учреждения убедиться в отсутствии в помещении посторонних лиц.

8. Для осуществления контроля и поддержания надлежащего режима обработки персональных должностное лицо Учреждения, ответственное за организацию обработки персональных, обязано систематически информировать должностных лиц, осуществляющих обработку защищаемой информации в ИСПДн, о необходимости повышения их бдительности и персональной ответственности.

Приложение № 4
к приказу 44/2 - ОД
от 06.09.2018 №

Правила
осуществления внутреннего контроля соответствия обработки персональных данных в информационной системе персональных данных в МОУ Ахматовская ООШ

Общие положения

Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее - Правила) в информационной системе персональных данных **МОУ Ахматовская ООШ**
(далее Учреждение) разработаны в соответствии с законодательством Российской Федерации и законодательством Тверской области и определяют порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

1. **Тематика внутреннего контроля.**

1.1. Тематика проверок обработки персональных данных с использованием средств автоматизации:

а) соответствие полномочий пользователя матрице доступа;

б) соблюдение пользователями информационной системы персональных данных (далее ИСПДн) Учреждения требований инструкции по организации парольной защиты в информационных системах персональных данных Учреждения;

в) соблюдение пользователями ИСПДн требований инструкции по организации антивирусной защиты в информационных системах персональных данных Учреждения;

г) соблюдение порядка доступа в помещения Учреждения, в которых ведется обработка персональных данных работников;

д) знание пользователями ИСПДн порядка своих действий во внештатных ситуациях.

1.2. Тематика проверок обработки персональных данных без использования средств автоматизации:

а) соблюдение правил хранения бумажных носителей с персональными данными;

б) соблюдение порядка доступа к бумажным носителям с персональными данными;

в) соблюдение порядка доступа в помещения, где обрабатываются и хранятся бумажные носители с персональными данными.

2. Порядок проведения внутренних проверок.

2.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в Учреждении организуется проведение периодических проверок условий обработки персональных данных в соответствии с планом проверок (приложение №1 к Правилам).

2.2. Проверки осуществляются комиссией, создаваемой приказом директора Учреждения.

2.3. Внутренние проверки проводятся по необходимости, в соответствии с поручением директора Учреждения, но не реже одного раза в год.

2.4. Внутренние проверки осуществляются непосредственно на месте обработки персональных данных путем опроса, либо, при необходимости, путем осмотра рабочих мест работников, участвующих в процессе обработки персональных данных.

2.5. По результатам каждой проверки составляется Протокол проведения внутренней проверки (приложение №2 к Правилам).

2.6. При выявлении в ходе проверки нарушений председателем комиссии в протоколе делается запись о мероприятиях по устранению нарушений и сроках исполнения.

2.7. Протоколы хранятся у Ответственного в течение текущего года. Уничтожение протоколов проводится Ответственным самостоятельно в первом квартале года, следующего за отчетным.

2.8. О результатах проверки и мерах, необходимых для устранения нарушений, директору Учреждения докладывает председатель комиссии.

Приложение № 5
к приказу 44/2-ОД
от 06.09.2018. №

Должностная инструкция
ответственного за организацию обработки персональных данных в информационной системе персональных данных МОУ Ахматовская ООШ

Общие положения.

Ответственный за организацию обработки персональных данных в МОУ Ахматовская ООШ (далее – Учреждение) назначается из числа сотрудников приказом Директора и отвечает за организацию обработки персональных данных в информационной системе персональных данных (далее – ИСПДн) Учреждения.

Ответственный, в рамках исполнения обязанностей по организации обработки персональных данных подчиняется непосредственно директору Учреждения и осуществляет организацию и контроль соответствия обработки персональных данных установленным требованиям к защите персональных данных в Учреждении, нормативным и организационно-распорядительным документам по обеспечению безопасности персональных данных при их обработке в ИСПДн Учреждения.

1.1 Методическое руководство работой ответственного за организацию обработки персональных данных осуществляется уполномоченным областным исполнительным органом государственной власти Тверской области в сфере защиты информации.

1.2 Ответственный за организацию обработки персональных данных в своей работе руководствуется федеральным законодательством РФ, положениями, руководящими и нормативными документами ФСТЭК России и ФСБ России по защите информации и организационно-распорядительными документами для ИСПДн и несет персональную ответственность за свои действия.

1.3 Техническое обслуживание ИСПДн, проводятся под контролем ответственного за организацию обработки персональных данных.

1. Обязанности ответственного за организацию обработки персональных данных.

Ответственный обязан:

а) знать и выполнять правила обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории

субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований;

б) знать и выполнять действующие нормативные и руководящие документы, а также внутренние инструкции и распоряжения, регламентирующие порядок действий по обработке и защите персональных данных;

в) обеспечивать выполнение режимных и организационных мероприятий на месте эксплуатации ИСПДн, а также следить за выполнением требований по условиям размещения средств вычислительной техники и их сохранностью;

г) осуществлять ознакомление сотрудников Учреждения, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных (в том числе с требованиями к защите персональных данных), локальными актами по вопросам обработки персональных данных;

д) организовывать обучение сотрудников Учреждения, непосредственно осуществляющих обработку персональных данных;

е) принимать правовые, организационные и технические меры по обеспечению безопасности персональных данных при их обработке, предусмотренные соответствующими нормативными правовыми актами, для выполнения установленных Правительством Российской Федерации требований к защите персональных данных при их обработке, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

ж) в целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям организовывать проведение периодических проверок условий обработки персональных данных в ИСПДн Учреждения;

з) докладывать о результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, директору Учреждения;

и) проводить периодический контроль принятых организационных мер, направленных на исключение несанкционированного доступа в помещение.

2. Права ответственного за организацию обработки персональных данных.

Ответственный имеет право:

а) требовать от сотрудников Учреждения выполнения установленной технологии обработки персональных данных, инструкций и других нормативных правовых документов по обеспечению безопасности персональных данных;

б) участвовать в разработке мероприятий Учреждения по совершенствованию безопасности персональных данных;

в) инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения безопасности персональных данных, несанкционированного доступа, утраты, порчи защищаемых персональных данных и программных и аппаратных средств из состава ИСПДн;

г) обращаться к директору Учреждения с предложением о приостановке процесса обработки персональных данных или отстранению от работы сотрудников в случаях нарушения установленной технологии обработки персональных данных или нарушения режима конфиденциальности;

д) подавать свои предложения по совершенствованию правовых, организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн Учреждения.

Приложение № 10
к приказу 44/2-ОД
от 06.09.2018 №

Инструкция
по применению парольной защиты и личных идентификаторов в информационной системе персональных данных МОУ Ахматовская ООШ

Общие положения.

Настоящая инструкция определяет требования к порядку использования, генерации, смены и прекращения действия паролей и личных идентификаторов пользователей информационной системы персональных данных (далее – ИСПДн МОУ Ахматовская ООШ

1.1 (далее – Учреждение) и устанавливает ответственность сотрудников Учреждения, эксплуатирующих и сопровождающих ИСПДн, за их выполнение, а также к контролю действий пользователей при работе с паролями.

1.2 Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей, а также контроль действий пользователей при работе с паролями возлагается на администратора безопасности информации ИСПДн.

1.3 Пароли для всех учетных записей пользователей ИСПДн должны выбираться с учетом следующих требований:

– длина пароля должна быть не менее 6 буквенно-цифровых символов;

– пароль не должен включать в себя легко вычисляемые (угадываемые) сочетания символов (имена, фамилии, отчества, наименования организации и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER, ADM, ADMIN и т.п.);

– максимальное действие пароля - не более чем 90 дней;

– пароль не должен повторяться;

– пользователь не может неправильно ввести пароль учетной записи более 5 раз, в этом случае должна происходить блокировка учетной записи пользователя, до момента снятия блокировки.

1.4 Для генерации «стойких» значений паролей могут применяться специальные программные средства.

1.5 При первичной регистрации пользователя в ИСПДн пароль ему назначает администратор безопасности информации.

1.6 Пользователи ИСПДн обязаны хранить свой личный пароль втайне от других и не передавать любым способом пароль третьим лицам.

1.7 Пользователь ИСПДн лично должен проводить смену пароля учетной записи регулярно не реже одного раза в три месяца.

1.8 Привязку идентификатора к пользователю (учетной записи) выполняет администратор безопасности информации.

1.9 Пользователи ИСПДн получают свой идентификатор у администратора безопасности информации.

1.10 Пользователь ИСПДн обязан хранить свой личный идентификатор в недоступных для других сотрудников хранилищах.

1.11 Пользователю ИСПДн запрещается передавать свой личный идентификатор.

1.12 В случае утери личного идентификатора, пользователь ИСПДн должен немедленно доложить об этом администратору безопасности информации.

1.13 При наличии технологической необходимости использования имен и паролей сотрудников в их отсутствие (например, в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п.), пароли данных сотрудников должны быть незамедлительно изменены администратором безопасности информации.

1.14 Полная плановая смена паролей пользователей должна проводиться регулярно, но не реже одного раза в год.

1.15 В случае прекращения полномочий учетной записи пользователя ИСПДн (увольнение, переход на другую работу, в другой отдел или помещение, а также другие обстоятельства) учетная запись должна быть удалена, а её идентификатор должен быть сдан администратору безопасности информации после окончания последнего сеанса работы данного пользователя в ИСПДн.

1.16 Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и другие обстоятельства) администратора безопасности информации.

1.17 В случае компрометации личного пароля или утери личного идентификатора пользователя администратором безопасности информации должны быть немедленно предприняты меры в соответствии с п. 1.18 настоящей Инструкции.

1.18 Администратор безопасности информации должен провести служебное расследование для выяснения причин компрометации пароля с целью выработки новых или совершенствования принятых технических и организационных мер по устранению такой угрозы в будущем, а также выяснению величины ущерба, который может быть нанесен собственнику информационных ресурсов.

Доведение Инструкции до сотрудников Учреждения. в части их касающейся осуществляется администратором безопасности информации ИСПДн под роспись в Листе ознакомления с данной инструкцией

Приложение № 11
к приказу 244/2-ОД
от 06.09.2018 №

Регламент
резервного копирования и восстановления персональных данных в информационной системе персональных данных МОУ Ахматовская ООШ

1. Общие положения.

1.1 Настоящий Регламент разработан с целью:

– определения порядка резервирования данных для последующего восстановления работоспособности информационной системы персональных данных (далее – ИСПДн) **МОУ Ахматовская ООШ** (далее – Учреждение) при полной или частичной потере информации, вызванной сбоями или отказами аппаратного или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.);

– определения порядка восстановления информации в случае возникновения такой необходимости;

– упорядочения работы сотрудников Учреждения связанной с резервным копированием и восстановлением информации.

1.2 В настоящем документе определяются действия при выполнении следующих мероприятий:

– резервное копирование;

– контроль резервного копирования;

– хранение резервных копий;

– полное или частичное восстановление данных и приложений.

1.3 Резервному копированию подлежит информация в электронном виде, согласно «Перечню информации, обрабатываемой в ИСПДн».

1.4 Настоящая инструкция определяет требования к организации учета, хранения и выдачи машинных носителей, содержащих персональные данные в ИСПДн.

1.5 Учет, хранение и выдачу машинных носителей персональных данных осуществляет ответственный за обеспечение безопасности персональных данных в ИСПДн, который несет личную ответственность за сохранность персональных данных. При увольнении сотрудника, ответственного за учет, хранение и выдачу машинных носителей персональных данных, составляется акт приема-сдачи этих документов, который утверждается директором Учрежения.

1.6 Доведение Инструкции до сотрудников Учреждения в части их касающейся осуществляется администратором безопасности информации под роспись в Листе ознакомления с данной инструкцией.

2. Порядок резервного копирования.

2.1 Резервное копирование информации производится на основании следующих данных:

– состав и объем копируемых данных, периодичность проведения резервного копирования;

– максимальный срок хранения резервных копий;

2.2 Система резервного копирования должна обеспечивать производительность, достаточную для сохранения информации, в установленные сроки и с заданной периодичностью.

2.3 О выявленных попытках несанкционированного доступа к резервируемой информации, а также иных нарушениях информационной безопасности, произошедших в процессе резервного копирования, сообщается ответственному за обеспечение безопасности персональных данных.

3. Методика резервного копирования.

Резервное копирование осуществляется средствами ОС Windows путем копирования информации на несъемный жесткий диск.

4. Контроль результатов резервного копирования.

4.1 Контроль результатов всех процедур резервного копирования осуществляется ответственным за эксплуатацию ИСПДн в срок до 17 часов рабочего дня, следующего за установленной датой выполнения этих процедур.

4.2 В случае обнаружения ошибки администратор безопасности информации сообщает об этом факте ответственному за обеспечение безопасности персональных данных до 18 часов текущего рабочего дня.

4.3 На протяжении периода времени, когда система резервного копирования находится в аварийном состоянии, должно осуществляться ежедневное копирование информации, подлежащей резервированию, с использованием средств файловых систем серверов, располагающих необходимыми объемами дискового пространства для её хранения.

5. Ротация носителей резервной копии.

5.1 Система резервного копирования должна обеспечивать возможность периодической замены (выгрузки) резервных носителей без потерь информации на них, а также обеспечивать восстановление текущей информации автоматизированных систем в случае отказа любого из устройств резервного копирования.

5.2 Все процедуры по загрузке, выгрузке носителей из системы резервного копирования осуществляются ответственным за обеспечение безопасности персональных данных.

5.3 В качестве новых носителей допускается повторно использовать те, у которых срок хранения содержащейся информации истек.

5.4 Персональные данные с носителей, которые перестают использоваться в системе резервного копирования, должны стираться.

6. Ротация носителей резервной копии.

6.1 В случае необходимости восстановление данных из резервных копий производится на основании Заявки владельца информации, согласованной с ответственным за обеспечение безопасности персональных данных.

6.2 После поступления заявки восстановление данных осуществляется в максимально сжатые сроки, ограниченные техническими возможностями системы, но не более одного рабочего дня.

Приложение № 14
к приказу 44/2 - ОД
от 06.09.2018. №

Правила
рассмотрения запросов субъектов персональных данных или их представителей

1. Субъекты персональных данных или их представители имеют право обращаться в **МОУ Ахматовская ООШ** (далее – Учреждение) для получения информации, касающейся обработки их персональных данных, в том числе содержащей:
   - подтверждение факта обработки персональных данных;
   - правовые основания и цели обработки персональных данных;
   - цели и применяемые способы обработки персональных данных;
   - сведения о лицах, которые имеют доступ к персональным данным в Учреждении;
   - сроки обработки персональных данных, в том числе сроки их хранения;
   - обрабатываемые персональные данные, относящиеся к данному субъекту персональных данных;
   - иные сведения, предусмотренные законодательством Российской Федерации в области персональных данных.
2. Субъект персональных данных вправе требовать от Учреждения 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.
3. Сведения, указанные в пункте 1 настоящих Правил, должны быть предоставлены в доступной форме и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.
4. Сведения, указанные в пункте 1 настоящих Правил, предоставляются субъекту персональных данных или его представителю ответственным за организацию обработки персональных данных в Учреждении, после получения письменного запроса от субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, подпись субъекта или его представителя.
5. В случае, если запрашиваемые сведения, были предоставлены для ознакомления субъекту персональных данных по его запросу, он вправе

обратиться повторно в Учреждение для получения указанных сведений и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения.

6. Субъект персональных данных или его представитель вправе обратиться повторно в Учреждениие для получения сведений, указанных в пункте 1 настоящих Правил, а также в целях ознакомления с обрабатываемыми его персональными данными до истечения срока, указанного в пункте 5 настоящих Правил, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в пункте 4 настоящих Правил, должен содержать обоснование направления повторного запроса.

7. Учреждение вправе отказать субъекту персональных данных или его представителю в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 5 и 6 настоящих Правил. Такой отказ должен быть мотивированным.

8. Право субъекту персональных данных или его представителю на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе, если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

Заведующей
МДОУ Детский сад № 1п.Молоково
Фадеевой Г.А.

от _____
паспорт _____
проживающего(ей) по адресу: _____
контактный телефон: _____

СОГЛАСИЕ
на обработку персональных данных воспитанника

Я, _____ в соответствии с пунктом 1 части 1 статьи 6 и статьи 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» своей волей и в своих интересах даю согласие *МДОУ Детский сад № 1* п.Молоково зарегистрированному по адресу: Тверская обл. п.Молоково ул.Ленина д9А, *ОГРН 1026901538476, ИНН 6906007648*, на обработку персональных данных моего ребенка, _____, _____ 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;
- сведения о родителях, законных представителях (фамилия, имя, отчество, дата и место рождения, пол, гражданство, должность, место работы, адреса, номера телефонов, 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, ребенок-сирота);
- сведения о состоянии здоровья (группа здоровья, инвалидность, хронические заболевания, прививки);
- информация, указанная в портфолио воспитанника;
- фотографии;

с целью предоставления льгот, гарантий и компенсации по оплате услуг *МДОУ Детский сад № 1*п.Молоково

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 *МДОУ Детский сад № 1п.Молоково* об изменении персональных данных _____ в течение месяца после того, как они изменились.
Об ответственности за предоставление недостоверных персональных данных пре-дупреждена.
Подтверждаю, что ознакомлена с документами *МДОУ Детский сад № 1*п.Молоково устанавливающими порядок обработки персональных данных, а также с моими правами и обязанностями.
Предупреждена, что согласие на обработку персональных данных может быть отозвано мною путем направления *МДОУ Детский сад № 1п.Молоково* письменного отзыва.
Настоящее согласие действует со дня его подписания до момента отчисления _____ из *МБДОУ Детский сад № 1*п.Молоково

подпись

число