РАССМОТРЕНО
протокол общего собрания
№ 3 от 29.05.2020 г.

УТВЕРЖДЕНО
директор МАОУ «СОШ № 134» г.Перми
_____ О.А. Ростовщикова
приказ № 059-08/121-134-01/4-96 от 01.06.2020 г.

# ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МАОУ «СОШ № 134» г.Перми

## 1. Общие положения

1.1. Политика информационной безопасности МАОУ «СОШ № 134» г.Перми (далее - школа) определяет цели и задачи системы обеспечения информационной безопасности и устанавливает совокупность правил, процедур, практических приемов, требований и руководящих принципов в области информационной безопасности, которыми руководствуются работники школы при осуществлении своей деятельности.

1.2. Настоящая Политика информационной безопасности определяет в школе цели и задачи защиты информации, устанавливает методы защиты информации от случайного или преднамеренного изменения, раскрытия или уничтожения, а также в целях соблюдения конфиденциальности, целостности и доступности информации, обеспечения процесса автоматизированной обработки данных в управлении, которыми должны руководствоваться педагогические и иные работники школы, при обработке информации в электронном виде, в том числе в информационных системах, а также ответственность работников за нарушение требований настоящей Политики информационной безопасности.

1.3. Политика информационной безопасности разработана в соответствии с правовыми требованиями Конституции Российской Федерации, Гражданского кодекса Российской Федерации, Уголовного кодекса Российской Федерации, Кодекса Российской Федерации об административных правонарушениях, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите и информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи», Указом Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера», Постановлением Правительства РФ № 781 от 17.1107 г. «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», Постановлением Правительства РФ № 687 от 15.09.08 г. «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», а также рядом иных нормативных правовых актов в сфере защиты информации.

1.4. Выполнение требований Политики информационной безопасности является обязательным для всех сотрудников школы.

1.5. Ответственность за соблюдение информационной безопасности несет каждый сотрудник школы. На лиц, работающих по договорам гражданско-правового характера, положения настоящей Политики распространяются в случае, если это обусловлено в таком договоре.

1.6. В настоящей Политике информационной безопасности используются следующие термины и определения:

- вирус (компьютерный, программный) - исполняемый программный код или интерпретируемый набор инструкции, обладающий свойствами несанкционированного распространения и самовоспроизведения;

- вредоносная программа - программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных;

- доступность информации - состояние информации, при котором субъекты, имеющие санкционированные права доступа, могут реализовать их беспрепятственно;

- защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии требованиями правовых документов или требованиями, устанавливаемыми собственником информации;

- идентификатор (имя, логин) - набор символов, представляющий уникальное наименование объекта или субъекта в информационной системе, позволяющее однозначно идентифицировать пользователя при входе его в систему, определить его права в ней, фиксировать действия и тому подобное;

- информационная безопасность - состояние защищенности информационной среды;

- информационная среда - совокупность условий для технологической переработки и эффективного использования информационных ресурсов (в том числе технические средства, программное обеспечение, телекоммуникации, уровень подготовки пользователей, формы контроля, документопотоки, процедуры, регламенты, юридические нормы, иные факторы, воздействующие на информационные процессы и информационные системы);

- информационные ресурсы - отдельные документы, массивы документов, в том числе содержащиеся в информационных системах (архивах, фондах, банках данных, других информационных системах);

- инцидент информационной безопасности - любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность;

- несанкционированное действие - действие субъекта в нарушение установленных в информационной системе регламентируемых правил обработки информации;

- пароль - конфиденциальная последовательность символов, связанная с субъектом и известная только ему, позволяющая его аутентифицировать, то есть подтвердить соответствие реальной сущности субъекта предъявляемому им при входе идентификатору;

- профиль - набор установок и конфигураций, специфичный для данного субъекта или объекта и определяющий его работу в информационной системе;

- системный администратор - лицо, обеспечивающее выполнение функций по обеспечению работы компьютерной техники, сети и программного обеспечения в школе;

- угроза безопасности информации - потенциально возможное событие, действие, процесс или явление, которое может привести к нарушению конфиденциальности, целостности, доступности информации, а также неправомерному тиражированию, которое наносит ущерб собственнику, владельцу или пользователю информации;

- уязвимость - свойство информационной системы, обусловливающее возможность реализации угроз безопасности, обрабатываемой в ней информации;

- целостность информации - состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими санкционированное право на изменение информации.

Термины «информация, информационная система, информационная система персональных данных, конфиденциальность информации, обладатель информации, сайт в сети Интернет (далее - сайт), спам, обезличивание персональных данных, общедоступная информация» используются в значениях, установленных Федеральными законами от 27 июля 2006 г, № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27 июля 2006 г, № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 10 сентября 2007 г. № 575 «Об утверждении Правил оказания телематических услуг связи».

## 2. Цель и задачи политики информационной безопасности

2. 1. Основными целями политики информационной безопасности в школе являются:
- сохранение конфиденциальности критичных информационных ресурсов;
- обеспечение непрерывности доступа к информационным ресурсам школы;
- защита целостности информации с целью поддержания возможности школы по оказанию услуг высокого качества и принятию эффективных управленческих решений;
- повышение осведомленности пользователей в области рисков, связанных с информационными ресурсами школы;
- выявление и оценка потенциальных угроз информационной безопасности и уязвимостей объектов защиты;
- определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности;
- исключение либо минимизация выявленных угроз безопасности;
- предотвращение инцидентов информационной безопасности;
- повышение уровня эффективности, непрерывности, контролируемости мер по защите от реальных угроз информационной безопасности;
- предотвращение и/или снижение ущерба от инцидентов информационной безопасности.

2.2 Основными задачами политики информационной безопасности в школе являются:
- разграничение доступа к техническим средствам и информационным ресурсам школы;
- регламентация работы в сети Интернет;
- разработка требований по обеспечению информационной безопасности;
- контроль выполнения установленных требований по обеспечению информационной безопасности;
- повышение эффективности, непрерывности, контролируемости мероприятий по обеспечению и поддержанию информационной безопасности;
- разработка нормативных документов для обеспечения информационной безопасности школы;
- выявление, оценка, прогнозирование и предотвращение реализации угроз информационной безопасности школы;
- организация антивирусной защиты информационных ресурсов школы;
- защита информации школы от несанкционированного доступа и утечки по техническим каналам связи;
- организация внутреннего контроля соблюдения информационной безопасности и обучение работников школы с последующим представлением отчета по результатам директору школы.

## 3. Концептуальная схема обеспечения информационной безопасности

3.1. Политика информационной безопасности школы направлена на защиту информационных ресурсов (активов) от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий сотрудников школы, технических сбоев автоматизированных систем, неправильных технологических и организационных решений в процессах поиска, сбора хранения, обработки, предоставления и распространения информации и обеспечение эффективного и бесперебойного процесса деятельности.

3.2. Наибольшими возможностями для нанесения ущерба обладает собственный персонал школы. Риск аварий и технических сбоев в автоматизированных системах определяется состоянием аппаратного обеспечения, надежностью систем энергоснабжения и телекоммуникаций, квалификацией сотрудников и их способностью к адекватным и

незамедлительным действиям в нештатных ситуации.

3.3. Стратегия обеспечения информационной безопасности школы заключается в использовании заранее разработанных мер противодействия атакам злоумышленников. А также программно-технических и организационных решений, позволяющих свести к минимуму возможные потери от технических аварий и ошибочных действий сотрудников школы.

## 4. Основные принципы обеспечения информационной безопасности

4.1. основными принципами обеспечения информационной безопасности являются:
- постоянный и всесторонний анализ автоматизированных систем и трудового процесса с целью выявления уязвимости информационных активов школы;
- своевременное обнаружение проблем, потенциально способных повлиять на информационной безопасности школы, корректировка моделей угроз и нарушителя;
- разработка и внедрение защитных мер;
- контроль эффективности принимаемых защитных мер;
- персонификация и разделение ролей и ответственности между сотрудниками школы за обеспечение информационной безопасности школы исходит из принципа персональной и единоличной ответственности за совершаемые операции.

## 5. Объекты защиты

5.1.Объектами защиты с точки зрения информационной безопасности являются:
- информационный процесс профессиональной деятельности;
- информационные активы школы.

5.2.Зашищаемая информация делится на следующие виды:
- информация по финансово-экономической деятельности школы;
- персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес,
семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;
- другая информация, не относящаяся ни к одному из указанных выше видов, которая отмечена грифом «Для служебного пользования» или «Конфиденциально».

## 6. Требования по информационной безопасности

6.1. В отношении всех собственных информационных активов школы должна быть определена ответственность соответствующего сотрудника школы. Информация о смене владельцев активов, их распределении, изменениях в конфигурации и использовании за пределами школы должна доводиться до сведения директора школы.

6.2. Все работы в пределах школы должны выполняться в соответствии с официальными должностными обязанностями только на компьютерах, разрешенных к использованию.

6.3. Ответственные сотрудники должны периодически пересматривать права доступа работников школы и других пользователей к соответствующим информационным ресурсам.

6.4. В целях обеспечения санкционированного доступа к информационному ресурсу, любой вход в  должен осуществляться с использованием уникального имени пользователя и пароля.

6.5. Пользователи должны руководствоваться рекомендациями по защите своего пароля на этапе его выбора и последующего использования. Запрещается сообщать свой пароль другим лицам или предоставлять свою учетную запись другим, в том числе членам своей семьи и близким.

6.6. Доступ к сети Интернет обеспечивается только в учебно-методических целях и не может использоваться для незаконной деятельности.

Рекомендованные правила:

- сотрудникам школы разрешается использовать сеть Интернет только в образовательных целях;
- запрещается посещение любого сайта в сети Интернет, который считается оскорбительным для общественного мнения, содержит информацию сексуального или террористического характера, пропаганду расовой ненависти, комментарии по поводу различия/превосходства полов, дискредитирующие заявления или иные материалы с оскорбительными высказываниями по поводу чьего-либо возраста, сексуальной ориентации, религиозных или политических убеждений, национального происхождения или недееспособности;
- работа сотрудников школы на персональных компьютерах допускается только под своей персональной учетной записью с ограниченными правами доступа уровня «Пользователь»;
- сотрудники школы перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов;
- запрещен доступ в Интернет через сеть школы для всех лиц, не являющихся сотрудниками школы, включая членов семьи сотрудников.

6.7. Ответственный работник (технический специалист, инженер) имеет право:

- осуществлять внесение изменений в систему ПК, настройку, установку необходимого ПО, администрирование записей пользователей под специальной учетной записью «Администратор»;
- контролировать содержание всего потока информации, проходящей через канал связи к сети Интернет в обоих направлениях;
- обучать сотрудников пользованию средствами антивирусного ПО, безопасным методам работы на ПК, с электронной почтой, в сети Интернет под подпись в листе ознакомления (прохождения обучения/инструктажа) либо журнале ознакомления (прохождения обучения/инструктажа) с указанием фамилии, имени, отчества служащего и даты ознакомления (прохождения обучения/проведения инструктажа);
- проверять перед утилизацией все компоненты оборудования, в состав которых входят носители данных (включая жесткие диски), чтобы убедиться в отсутствии на них конфиденциальных данных и лицензионных продуктов. Должна выполняться процедура форматирования носителей информации, исключающая возможность восстановления данных.

6.8. Сотрудники должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранится информация школы.

6.9. Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения,

6.10. Все компьютерное оборудование (серверы, стационарные и портативные компьютеры), периферийное оборудование (например, принтеры и сканеры), аксессуары (манипуляторы типа «мышь», шаровые манипуляторы, дисководы для CD-дисков), коммуникационное оборудование (факс-модемы, сетевые адаптеры, концентраторы и пр.), для целей настоящей политики вместе именуются «компьютерное оборудование». Компьютерное оборудование, предоставленное школой, является ее собственностью и предназначено для использования исключительно в образовательных целях.

6.11. Каждый сотрудник, получивший в пользование портативный компьютер, обязан принять надлежащие меры по обеспечению его сохранности.

6.12. Все компьютеры должны защищаться паролем при загрузке системы, активации по горячей клавиши и после выхода из режима «Экранной заставки». Для установки режимов зашиты пользователь должен обратиться к администратору. Данные не должны быть скомпрометированы в случае халатности или небрежности приведшей к потере оборудования.

6.13. При записи какой-либо информации на носитель для передачи субъектам, участвующим в информационном обмене, необходимо убедиться в том, что носитель чист, то есть не содержит никаких иных данных. Простое переформатирование носителя не дает гарантии полного удаления записанной на нем информации.

6.14. Порты передачи данных, в том числе CD-дисководы в стационарных компьютерах сотрудников школы блокируются, за исключением тех случаев, когда сотрудником получено разрешение на запись от администратора.

6.15. Все программное обеспечение, установленное на предоставленном школой компьютерном оборудовании, является собственностью школы и должно использоваться исключительно в образовательных целях.

6.16. Сотрудникам запрещается устанавливать на предоставленном в пользование компьютерном оборудовании нестандартное, нелицензионное программное обеспечение или программное обеспечение, не имеющее отношения к их образовательной деятельности, если в ходе выполнения технического обслуживания будет обнаружено неразрешенное к установке программное обеспечение, то оно будет удалено, а сообщение о нарушении будет направлено директору школы.

- На всех портативных компьютерах должны быть установлены программы необходимые для обеспечения защиты информации, в т.ч. антивирусное программное обеспечение;

6.17. Сотрудники школы не должны:

- допускать отключение установленного антивирусного ПО или отказ от обновления антивирусных баз, блокировать антивирусное программное обеспечение;
- устанавливать другое антивирусное программное обеспечение;
- изменять настройки и конфигурацию антивирусного программного обеспечения,

6.18. Электронные сообщения должны строго соответствовать стандартам в области деловой этики. Использование корпоративной электронной почты в личных целях не допускается. Сотрудникам запрещается направлять конфиденциальную информацию школы по электронной почте. Строго конфиденциальная информация школы, ни при каких обстоятельствах, не подлежит пересылке третьим лицам по электронной почте.

6.19. Использование сотрудниками школы публичных почтовых ящиков электронной почты осуществляется только при согласовании с ответственным за обеспечение безопасности информации.

6.20. Сотрудники школы для обмена документами должны использовать только свой официальный адрес корпоративной электронной почты.

6.21. Сообщения, пересылаемые по электронной почте, представляют собой постоянно используемый инструмент для электронных коммуникаций, имеющих тот же статус, что и письма и факсимильные сообщения. Электронные сообщения подлежат такому же утверждению и хранению, что и прочие средства письменных коммуникаций.

В целях предотвращения ошибок при отправке сообщений пользователи перед отправкой должны внимательно проверить правильность написания имен и адресов получателей. В случае получения сообщения лицом, вниманию которого это сообщение не предназначается, такое сообщение необходимо переправить непосредственному получателю.

6.22. Не допускается при использования корпоративной электронной почты:

- рассылка сообщений личного характера, использующих значительные ресурсы электронной почты;
- рассылка рекламных материалов;

- подписка на рассылку, участие в дискуссиях и подобные услуги, использующие значительные ресурсы электронной почты в личных целях;
- поиск и чтение сообщений, направленных другим лицам (независимо от способа их хранения);
- пересылка любых материалов, как сообщений, так и приложений, содержание которых является противозаконным, непристойным, злонамеренным, оскорбительным, угрожающим, клеветническим, злобным или способствует поведению, может рассматриваться как уголовное преступление или административный проступок либо приводит к возникновению гражданско-правовой ответственности, беспорядков или противоречит стандартам в области этики.

6.23. Все пользователи должны быть осведомлены о своей обязанности сообщать об известных или подозреваемых ими нарушениях информационной безопасности, а также должны быть проинформированы о том, что ни при каких обстоятельствах они не должны пытаться использовать ставшие им известными слабые стороны системы безопасности.

6.24. В случае кражи переносного компьютера следует незамедлительно сообщить администратору и/или директору школы.

6.25. Если имеется подозрение или выявлено наличие вирусов или иных разрушительных компьютерных кодов, то сразу после их обнаружения сотрудник обязан:
- проинформировать администратора;
- не использовать и не включать зараженный компьютер;
- не подсоединять этот компьютер к компьютерной сети школы до тех пор, пока на нем не будет произведено удаление обнаруженного вируса и полное антивирусное сканирование администратором.

6.26. Участникам заседаний запрещается входить в помещения с записывающей аудио/видео аппаратурой, фотоаппаратами, диктофонами и мобильными телефонами без предварительного согласования с ответственным сотрудником или директором школы.

6.27. Аудио/видео запись, фотографирование во время конфиденциальных заседаний может вести только сотрудник школы, который отвечает за подготовку заседания, после получения письменного разрешения руководителя группы организации встречи.

6.28. Сотрудникам школы запрещается:
- нарушать информационную безопасность и работу сети школы;
- получать доступ к компьютеру, сети или учетной записи в обход системы идентификации пользователя или безопасности;
- передавать информацию о сотрудниках или списки сотрудников школы посторонним лицам;
- создавать, обновлять или распространять компьютерные вирусы и прочие разрушительное программное обеспечение.

6.29. Ответственность за сохранность данных на стационарных и портативных персональных компьютерах лежит на пользователях.

6.30. Необходимо регулярно, не менее одного раза в четверть, делать резервные копии всех основных служебных данных и используемого программного обеспечения.

6.31. Все заявки на проведение технического обслуживания компьютеров должны направляться администратору письменно через «Журнал заявок на обслуживание компьютерной техники».

6.32. Все операционные процедуры и процедуры внесения изменений в информационные системы и сервисы должны быть документированы и согласованны с администратором.

## 7. Управление информационной безопасностью

7.1 .Управление информационной безопасности школы включает в себя:
- разработку и поддержание в актуальном состоянии Политики информационной безопасности;

- разработку и поддержание в актуальном состоянии нормативно-методических документов по обеспечению информационной безопасности;
- обеспечение бесперебойного функционирования комплекса средств информационной безопасности;
- осуществление контроля (мониторинга) функционирования системы информационной безопасности;
- оценку рисков, связанных с нарушениями информационной безопасности.

## 8. Реализация политики информационной безопасности

Реализация Политики информационной безопасности школы осуществляется на основании документов, регламентирующих отдельные процедуры и процессы профессиональной деятельности в управлении.

## 9. Порядок внесения изменений и дополнений в политику информационной безопасности

Внесение изменений и дополнений в Политику информационной безопасности производится не реже одного раза в три года с целью приведения в соответствие определенных Политикой защитных мер реальным жизненным условиям и текущим требованиям к защите информации.

## 10. Контроль за соблюдением Политики информационной безопасности

10.1. Текущий контроль за соблюдением выполнения требований Политики информационной безопасности школы возлагается на сотрудника, назначенного приказом директора школы.

10.2. Директор школы на регулярной основе рассматривает реализацию и соблюдение отдельных положений Политики информационной безопасности, а также осуществляет последующий контроль за соблюдением ее требований.

## 11. Ответственность за нарушения настоящей Политики информационной безопасности

Работники школы в рамках должностных обязанностей и полномочий несут ответственность в соответствии с действующим законодательством Российской Федерации за:
- невыполнение требований настоящей Политики информационной безопасности;
- действия или бездействие, ведущие к нарушению информационной безопасности школы;
- действия или бездействие, ведущие к нарушению действующего законодательства Российской Федерации в области информационных технологий.