Принято
На педагогическом совете
Протокол № 1
«26» августа 2015 г.

Утверждаю:
Директор МБОУ «СОШ №2»
_____ В.А.Гавриленко
пр.№ 473 от «31» августа 2015 г.

ПРАВИЛА (регламент)
по работе в локальной сети и сети Интернет
муниципального бюджетного образовательного учреждения «Средняя общеобразовательная школа № 2» г. Назарово Красноярского края

Персональные компьютеры, серверы, программное обеспечение, вся информация, хранящаяся на них и вновь создаваемая, оборудование локальной вычислительной сети, коммуникационное оборудование являются собственностью муниципального бюджетного образовательного учреждения «Средняя общеобразовательная школа № 2» г. Назарово Красноярского края (в дальнейшем - школа) и предоставляются работникам и учащимся в рамках образовательной деятельности.

ПК, серверы, ПО, оборудование ЛВС и коммуникационное, пользователи образуют систему локальной компьютерной сети школы.

1. Общие положения.

1.1.Настоящий регламент является приложением к Положению о школьной локальной сети (далее - Сети).

1.2.Целью настоящего регламента является:

- регулирование работы системного администратора и пользователей;
- распределение сетевых ресурсов коллективного пользования и поддержание необходимого уровня защиты информации, ее сохранности и соблюдения прав доступа к информации;
- более эффективное использование сетевых ресурсов и уменьшение риска неправильного их использования.

1.3.К работе в Сети допускаются лица, прошедшие инструктаж

1.4.Работа в Сети каждому пользователю разрешена только на определенных компьютерах, в определенное время и только с разрешенными программами и сетевыми ресурсами. Если нужно работать вне указанного времени, на других компьютерах и с другими программами, необходимо получить разрешение системного администратора.

1.5.По уровню ответственности и правам доступа к Сети пользователи разделяются на следующие категории:

- системный администратор;
- пользователи-работники;
- пользователи-ученики.

1.6.Системный администратор является заместителем директора по информатизации и(или) лаборантом компьютерного класса. На него возлагается обязанность контролировать работоспособность Сети.

1.7.В случае появления у пользователя сведений или подозрений о фактах нарушения настоящих Правил, а в особенности о фактах несанкционированного удаленного доступа к информации, размещенной на контролируемом им компьютере или каком-либо другом, пользователь должен немедленно сообщить об этом системному администратору Сети.

1.8.Системный администратор - лицо, обслуживающее сервер и следящее за правильным функционированием Сети. Системный администратор дает разрешение на подключение компьютера к Сети, выдает IP-адрес компьютеру, создает учетную запись электронной почты для пользователя. Самовольное подключение своего компьютера к Сети является серьезнейшим нарушением правил пользования Сетью.

1.9.Пользователь-работник подключенного к Сети компьютера - работник школы, за которым закреплена ответственность за данный компьютер. Пользователь должен принимать все необходимые меры по защите информации и контролю за соблюдением прав доступа к ней.

1.10.Пользователи-ученики имеют доступ к компьютерам в компьютерных классах и компьютерам, установленным в читальном зале. В компьютерных классах за каждым учащимся закреплен определенный компьютер.

1.11.Каждый пользователь-работник пользуется индивидуальным именем пользователя и паролем для своей идентификации в локальной сети, выдаваемыми системным администратором. Имя пользователя и пароль для учащихся назначаются по номеру класса.

1.12.Каждый работник должен пользоваться только своим именем пользователя и паролем для входа в локальную сеть и сеть Интернет; передача их кому-либо запрещена. Для учащихся вход в локальную сеть определен именем пользователя internet.

1.13.В случае нарушения пользователем правил пользования Сетью, связанного с администрируемым им компьютером, он сообщает об этом системному администратору, который проводит расследование причин и принимает меры к пресечению подобных нарушений. Администратор имеет право отстранить виновника от пользования компьютером или принять иные меры.

1.14.Системный администратор информирует пользователей обо всех плановых профилактических работах, могущих привести к частичной или полной неработоспособности Сети на ограниченное время, а также об изменениях предоставляемых сервисов и ограничениях, накладываемых на доступ к ресурсам Сети.

1.15. Системный администратор имеет право отключить компьютер пользователя от Сети в случае, если с данного компьютера производились попытки несанкционированного доступа к информации на других компьютерах, а также при других серьезных нарушениях настоящих Правил.

1.16.Пользователь должен ознакомиться с инструкцией по работе на компьютере и в локальной сети. Обязанность ознакомления пользователя с инструкцией лежит на системном администраторе и заместителе директора по информатизации.

2. Работа на компьютере.

2.1.Перед началом работы пользователь должен:

• включить выключатель сетевого фильтра. При включении кнопка должна начать светиться;

• включить монитор (если выключен);

• включить компьютер кнопкой «Power». Дождаться загрузки операционной системы (ОС);

• войти в систему, используя свои личные имя пользователя и пароль.

2.2.По завершении работы пользователь должен:

• закрыть все открытые программы и документы, сохранив нужные изменения;

• с помощью меню «Пуск -» Завершение работы» выключить компьютер и дождаться завершения работы (системный блок перестанет мигать и шуметь);

• выключить монитор;

• выключить сетевой фильтр.

2.3. Запрещено аварийно завершать работу компьютера кнопкой «Reset» или отключением от электросети. Завершение работы компьютера производится через кнопку «Пуск -> Завершение работы».

2.4.Запрещается самостоятельно разбирать компьютер и все его комплектующие. При возникновении неисправностей необходимо обратиться к заведующему кабинета или заместителю директора по УВР, курирующему вопросы информатизации школы.

2.5.Все кабели, соединяющие системный блок с другими устройствами, следует вставлять и вынимать только при выключенном компьютере. Исключение составляют USB-устройства: они могут быть подключены' к включенному, компьютеру.

2.6.Подключение проектора к компьютеру осуществляется в выключенном состоянии. Выключить проектор из сети можно только после его полной остановки.

2.7.На компьютеры школы устанавливается программное обеспечение в соответствии с приобретенными лицензиями (или свободно распространяемое).

2.8.Запрещено самостоятельно устанавливать, удалять, деактивировать и изменять программное обеспечение и сетевые настройки на компьютере. Этим занимается системный администратор.

2.9.Пользователь обязан сохранять оборудование в целости и сохранности. Запрещается подвергать компьютер и периферийные устройства физическим, термическим и химическим воздействиям (нельзя сидеть на частях компьютера, проливать на них чай, кофе, просыпать семечки, ставить у батареи и других нагревательных приборов, класть книги, сумки и прочие предметы).

2.10.Системный блок компьютера должен стоять так, чтобы отверстия воздухозаборника не были закрыты.

2.11.По завершении рабочего дня компьютер необходимо выключить и обесточить.

2.12.Пользователь обязан помнить данные для входа на свой компьютер и в локальную сеть. В случае утраты этих данных необходимо обратиться к системному администратору.

3. Работа в локальной сети.

3.1. *Пользователи локальной сети (далее - Сеть) имеют право:*

• использовать в работе предоставленные им сетевые ресурсы в оговоренных рамках настоящих Правил. Системный администратор вправе ограничивать доступ к некоторым сетевым ресурсам вплоть до их полной блокировки, изменять распределение трафика и проводить другие меры,

направленные на повышение эффективности использования сетевых ресурсов;

• обращаться к администратору Сети по вопросам, связанным с распределением ресурсов компьютера. Какие-либо действия пользователя, ведущие к изменению объема используемых им ресурсов или влияющие на загруженность или безопасность системы (например, установка на компьютере коллективного доступа), должны санкционироваться системным администратором;

• обращаться за помощью к системному администратору при решении задач использования ресурсов Сети;

• вносить предложения по улучшению работы с ресурсом.

3.2. *Пользователи Сети обязаны:*

• соблюдать правила работы в Сети, оговоренные настоящим регламентом;

• при доступе к внешним ресурсам соблюдать правила, установленные системными администраторами для данных ресурсов;

• немедленно сообщать системному администратору Сети или заместителю директора по информатизации об обнаруженных проблемах в использовании предоставленных ресурсов, а также о фактах нарушения настоящих Правил кем-либо. Администратор (при необходимости - с помощью других специалистов) должен провести расследование указанных фактов и принять соответствующие меры;

• не разглашать известную им конфиденциальную информацию (имена пользователей, пароли), необходимую для безопасной работы в Сети;

• обеспечивать беспрепятственный доступ системного администратора к сетевому оборудованию и компьютерам пользователей для организации профилактических и ремонтных работ;

• выполнять предписания системного администратора, направленные на обеспечение безопасности Сети;

• в случае обнаружения неисправности компьютерного оборудования или программного обеспечения пользователь должен обратиться к системному администратору или заместителю директора, курирующего вопросы информатизации.

3.3. *Пользователям Сети запрещено:*

• разрешать посторонним лицам пользоваться вверенным им компьютером (кроме случаев подключения/отключения ресурсов, выполняемых системным администратором) без согласования с системным администратором;

• использовать сетевые программы, не предназначенные для выполнения их прямых служебных обязанностей, без согласования с заместителем директора;

• самостоятельно устанавливать или удалять установленные системным администратором сетевые программы на компьютерах, подключенных к Сети, изменять настройки операционной системы и приложений, влияющие на работу сетевого оборудования и сетевых ресурсов;

• повреждать, уничтожать или фальсифицировать информацию, не принадлежащую пользователю;

• вскрывать компьютеры, сетевое и периферийное оборудование; подключать к компьютеру дополнительное оборудование без согласования с

системным администратором, изменять настройки BIOS, а также производить загрузку рабочих станций со стороннего носителя информации;

• самовольно подключать компьютер к Сети, а также изменять IP-адрес компьютера, выданный системным администратором. Передача данных в Сеть с использованием других IP-адресов в качестве адреса отправителя является распространением ложной информации и создает угрозу безопасности информации на других компьютерах;

• работать с каналоемкими ресурсами (video, audio, chat и др.) без согласования с системным администратором Сети. При сильной перегрузке канала вследствие использования каналоемких ресурсов текущий сеанс пользователя, вызвавшего перегрузку, будет прекращен;

• получать и передавать в Сеть информацию, противоречащую действующему законодательству РФ и нормам морали, а также представляющую коммерческую или государственную тайну;

• обходить учетную систему безопасности, систему статистики, повреждать или дезинформировать ее;

• использовать иные формы доступа к сети Интернет, кроме тех, которые разрешены системным администратором (пытаться обходить межсетевой экран при соединении с сетью Интернет);

• осуществлять попытки несанкционированного доступа к ресурсам Сети, проводить или участвовать в сетевых атаках и сетевом взломе;

• использовать Сеть для массового распространения рекламы (спам), коммерческих объявлений, порнографической информации, призывов к насилию, разжиганию национальной или религиозной вражды, оскорблений, угроз и т. п.;

• закрывать доступ к информации паролями без согласования с системным администратором.

4. Работа с электронной почтой.

4.1.Электронная почта предоставляется сотрудникам школы только для выполнения их прямых служебных обязанностей. Использование ее в личных целях запрещено. Создание электронного почтового ящика проводится системным администратором после письменного распоряжения директора школы.

4.2.Все электронные письма, создаваемые и хранимые на компьютерах школы, являются собственностью школы и не считаются персональными.

4.3.Администрация школы (далее - школа) оставляет за собой право получить доступ к электронной почте сотрудников, если на то будут веские причины. Содержимое электронного письма не может быть раскрыто иначе как с целью обеспечения безопасности или по требованию правоохранительных органов.

4.4.Конфигурировать программы электронной почты пользователям разрешается лишь так, чтобы их стандартные действия, использующие установки по умолчанию, были бы наиболее безопасными.

4.5.Входящие письма должны проверяться на наличие вирусов или других вредоносных программ.

4.6.Справочники электронных адресов сотрудников не могут быть доступны всем и являются конфиденциальной информацией.

4.7.Пользователи не должны посылать сами или позволять кому-либо посылать письма от чужого имени.

4.8.Школа оставляет за собой право осуществлять наблюдение за почтовыми отправлениями сотрудников. Электронные письма могут быть прочитаны школой, даже если они были удалены и отправителем, и получателем, и при ненадлежащем содержании могут служить обоснованием наказания.

4.9.В качестве клиентов электронной почты могут использоваться только утвержденные почтовые программы.

4.10.Запрещается осуществлять массовую рассылку не согласованных предварительно электронных писем. Под массовой рассылкой подразумевается как рассылка множеству получателей, так и множественная рассылка одному получателю (спам).

5. Работа в сети Интернет.

5.1. Пользователи могут заниматься поиском информации в сети Интернет только в случае, если это необходимо для выполнения их должностных обязанностей.

5.2. Использование ресурсов сети Интернет разрешается только в рабочих и учебных целях; использование ее ресурсов не должно потенциально угрожать школе.

5.3.По использованию ресурсов сети Интернет ведется статистика и поступает в архив школы.

5.4.Действия любого пользователя, подозреваемого в нарушении правил пользования Интернетом, могут быть запротоколированы и применены для обоснования санкций в отношении данного лица.

5.5.Сотрудникам школы и учащимся, пользующимся Интернетом, запрещено передавать или загружать в Сеть материал, который является непристойным, порнографическим или нарушает действующее законодательство РФ**.**

5.6.Все программы, применяемые для доступа к сети Интернет, должны быть утверждены сетевым администратором и на них должны быть настроены необходимые уровни безопасности.

5.7. Запрещено получать и передавать через Интернет информацию, противоречащую законодательству РФ и нормам морали, представляющую коммерческую тайну, а также распространять информацию, задевающую честь и достоинство граждан; запрещено рассылать через сеть обманные, беспокоящие или угрожающие сообщения.

5.8. Запрещено получать доступ к информационным ресурсам Сети или сети Интернет, не являющимся публичными, без разрешения их собственника.

5.9. Системному администратору необходимо обеспечить в школе контентную фильтрацию ресурсов сети Интернет, вести список запрещенных сайтов. Программы для работы с Интернетом должны быть сконфигурированы так, чтобы к этим сайтам нельзя было получить доступ.

5.10. Запрещено размещать в гостевых книгах, форумах, конференциях сообщения, содержащие грубые и оскорбительные выражения.

6. Ответственность.

6.1. *Пользователь компьютера* отвечает за информацию, хранящуюся на его компьютере, а также за технически исправное состояние компьютера и другой вверенной техники.

6.2.*Системный администратор* отвечает за бесперебойное функционирование вверенной ему Сети, качество предоставляемых пользователям сервисов.

6.3.*Пользователь* несет личную ответственность за весь информационный обмен между его компьютером и другими компьютерами в Сети и за ее пределами.

6.4.За нарушение настоящего регламента *пользователь может быть отстранен* от работы с Сетью.

6.5.Нарушение кем-либо данного регламента, повлекшее уничтожение, блокирование, модификацию либо копирование охраняемой законом компьютерной информации, нарушение работы компьютеров пользователей, системы или Сети, может повлечь административную или уголовную ответственность в соответствии с действующим законодательством.