ПРИНЯТ
Общим собранием работников
МОБУ СОШ №20 имени Ф.К.Попова
ГО г. Якутск
Протокол № _1_ от «_1_» __09___ 2019 г.

УТВЕРЖДЕН
Приказом директора
МОБУ СОШ №20 имени Ф.К.Попова
ГО г. Якутск
№ 01-10/26 &1 от 05.09.2019

Правила
использования участниками образовательных отношений муниципального образовательного бюджетного учреждения
«Средняя общеобразовательная школа №20 имени Ф.К. Попова» ГО г. Якутск
сети Интернет

1. Общие положения

1.1. Настоящие Правила регламентируют условия и порядок использования сети Интернет через ресурсы МОБУ «СОШ №20 имени Ф.К. Попова» ГО г. Якутск.

1.2. Использование сети Интернет в образовательном учреждении направлено на решение задач учебно-воспитательной деятельности.

1.3. Правила регулируют условия и порядок использования сети Интернет в школе.

1.4. Настоящие Правила имеют статус локального нормативного акта образовательного учреждения.

2. Организация использования сети Интернет в общеобразовательном учреждении

2.1. Вопросы использования возможностей сети Интернет в учебно-образовательной деятельности рассматриваются на педагогическом совете школы. Педагогический совет утверждает Правила использования сети Интернет на учебный год. Правила вводятся в действие приказом руководителя школы.

2.2. Правила использования сети Интернет разрабатывается педагогическим советом ОУ на основе примерного регламента.

2.3. При разработке правил использования сети Интернет педагогический совет руководствуется:

- законодательством Российской Федерации;
- интересами обучающихся;
- целями образовательной деятельности;
- рекомендациями профильных органов и организаций в сфере классификации ресурсов Сети.

2.4. Для обеспечения доступа участников образовательных отношений к сети Интернет в соответствии с установленным в школе правилами руководитель школы назначает своим приказом ответственного за организацию работы с Интернетом и ограничение доступа.

2.5. Ответственный за организацию работы с Интернетом и ограничение доступа отвечает за обеспечение эффективного и безопасного доступа к сети Интернет в школе, а также за выполнение установленных правил.

2.6. Педагогический совет школы:

- принимает решение о разрешении/блокировании доступа к определенным ресурсам и (или) категориям ресурсов сети Интернет;

- определяет характер и объем информации, публикуемой на интернет-ресурсах школы;

- дает директору школы рекомендации о назначении и освобождении от исполнения своих функций лиц, ответственных за обеспечение доступа к ресурсам сети Интернет и контроль безопасности работы в Сети.

2.7. Во время уроков и других занятий в рамках учебного плана контроль использования обучающимися сети Интернет осуществляет педагог, ведущий занятие.

При этом педагог:

- наблюдает за использованием компьютера и сети Интернет обучающимися;

- принимает меры по пресечению обращений к ресурсам, не имеющим отношения к образовательной деятельности.

2.8. Во время свободного доступа обучающихся к сети Интернет вне учебных занятий, контроль использования ресурсов Интернета осуществляют работники школы, определенные приказом директора.

Работник образовательного учреждения:

- наблюдает за использованием компьютера и сети Интернет обучающимися;

- принимает меры по пресечению обращений к ресурсам, не имеющих отношения к образовательной деятельности;

- сообщает классному руководителю о преднамеренных попытках обучающегося осуществить обращение к ресурсам, не имеющим отношения к образовательной деятельности.

2.9. При использовании сети Интернет в школе обучающимся предоставляется доступ только к тем ресурсам, содержание которых не противоречит законодательству Российской Федерации и которые имеют прямое отношения к образовательной деятельности. Проверка выполнения такого требования осуществляется с помощью специальных технических средств и программного обеспечения контентной фильтрации, установленного в школе или предоставленного оператором услуг связи.

2.10. Отнесение определенных ресурсов и (или) категорий ресурсов в соответствующие группы, доступ к которым регулируется техническим средствами и программным обеспечением контентной фильтрации, в соответствии с принятыми в школе правилами обеспечивается работником школы, назначенным директором.

2.11. Принципы размещения информации на Интернет-ресурсах школы призваны обеспечивать:

- соблюдение действующего законодательства Российской Федерации, интересов и прав граждан;

- защиту персональных данных обучающихся, работников образовательного учреждения;

- достоверность и корректность информации.

2.12 Персональные данные обучающихся (включая фамилию и имя, класс/год обучения, возраст, фотографию, данные о месте жительства, телефонах и пр., иные сведения личного характера) могут размещаться на Интернет-ресурсах, создаваемых школой, по согласию родителей (законных представителей), которые были подписаны при поступлении в образовательное учреждение.

2.13. В информационных сообщениях о мероприятиях, размещенных на сайте школы без уведомления и получения согласия упомянутых лиц или их законных представителей, могут быть указаны лишь фамилия и имя обучающегося либо фамилия, имя и отчество преподавателя, сотрудника или родителя.

3. Использование сети Интернет в образовательном учреждении

3.1. Использование сети Интернет в школе осуществляется, как правило, в целях образовательной деятельности.

3.2. По разрешению лица, ответственного за организацию в школе работы сети Интернет и ограничение доступа, педагоги, сотрудники и обучающиеся вправе:

- размещать собственную информацию в сети Интернет на Интернет-ресурсах школы;
- иметь учетную запись электронной почты на Интернет-ресурсах школы.

3.3. Обучающиеся обязаны использовать сеть Интернет с разрешения лица, ответственного за организацию в школе работы сети Интернет и ограничение доступа или педагога.

3.4. Обучающемуся запрещается:

- обращаться к ресурсам, содержание и тематика которых не допустимы для несовершеннолетних и/или нарушают законодательство Российской Федерации (эротика, порнография, пропаганда насилия, терроризма, политического или религиозного экстремизма, национальной, расовой и т.п. розни, иные ресурсы схожей направленности);
- осуществлять любые сделки через Интернет;
- осуществлять загрузки файлов на компьютер школы без специального разрешения;
- распространять оскорбительную, не соответствующую действительности, порочащую других лиц информацию, угрозы.

3.4. При случайном обнаружении ресурса, содержание которого не имеет отношения к образовательной деятельности, обучающийся обязан незамедлительно сообщить об этом педагогу, проводящему занятие.

Педагог обязан зафиксировать адрес ресурса и время его обнаружения и сообщить об этом лицу, ответственному за работу локальной сети и ограничение доступа к информационным ресурсам. Ответственный обязан:

- принять информацию от преподавателя;
- направить информацию о некатегоризированном ресурсе технику-программисту и программного обеспечения технического ограничения доступа к информации (в течение суток);
- в случае явного нарушения обнаруженным ресурсом законодательства Российской Федерации сообщить о нем по специальной «горячей линии» для принятия мер в соответствии с законодательством Российской Федерации (в течение суток).

Передаваемая информация должна содержать:

- адрес ресурса;
- сообщение о тематике ресурса, предположения о нарушении ресурсом законодательства Российской Федерации либо его несовместимости с задачами образовательной деятельности;
- дату и время обнаружения;
- информацию об установленных в школе технических средствах технического ограничения доступа к информации.

Классификатор информации, распространение которой

запрещено в соответствии с законодательством Российской Федерации

№ п/п	Наименование тематической категории	Содержание
1	Пропаганда войны, разжигание ненависти и вражды, пропаганда порнографии и антиобщественного поведения	- информация, направленная на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды; - информация, пропагандирующая порнографию, культ насилия и жестокости, наркоманию, токсикоманию, антиобщественное поведение.
2	Злоупотребление свободой СМИ /экстремизм	информация, содержащая публичные призывы к осуществлению террористической деятельности, оправдывающая терроризм, содержащая другие экстремистские материалы
3	Злоупотребление свободой СМИ / наркотические средства	сведения о способах, методах разработки, изготовления и использования, местах приобретения наркотических средств, психотропных веществ и их прекурсоров, пропаганду каких-либо преимуществ использования отдельных наркотических средств, психотропных веществ, их аналогов и прекурсоров
4	Злоупотребление свободой СМИ / информация с ограниченным доступом	сведения о специальных средствах, технических приемах и тактике проведения контртеррористической операции
5	Злоупотребление свободой СМИ / скрытое воздействие	информация, содержащая скрытые вставки и иные технические способы воздействия на подсознание людей и (или) оказывающих вредное влияние на их здоровье
6	Экстремистские материалы или экстремистская деятельность (экстремизм)	А) экстремистские материалы, т.е. предназначенные для обнародования документы либо информация, призывающие к осуществлению экстремистской деятельности либо обосновывающие или оправдывающие необходимость осуществления такой деятельности, в том числе труды руководителей национал-социалистской рабочей партии Германии, фашистской партии Италии, публикации, обосновывающие или оправдывающие национальное и (или) расовое превосходство либо оправдывающие практику совершения военных или иных преступлений, направленных на полное или частичное уничтожение какой-либо этнической, социальной, расовой, национальной или религиозной группы; Б) экстремистская деятельность (экстремизм) включает в себя деятельность по распространению материалов (произведений), содержащих хотя бы один из следующих признаков: - насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации; - подрыв безопасности Российской Федерации; захват или присвоение властных полномочий; создание незаконных вооруженных формирований; - осуществление террористической деятельности либо публичное оправдание терроризма; - возбуждение расовой, национальной или религиозной розни, а также социальной розни, связанной с насилием или призывами к насилию; - унижение национального достоинства; осуществление массовых беспорядков, хулиганских действий и актов вандализма по мотивам идеологической, политической,

№ п/п	Наименование тематической категории	Содержание
		расовой, национальной или религиозной ненависти либо вражды, а равно по мотивам ненависти либо вражды в отношении какой-либо социальной группы; - пропаганду исключительности, превосходства либо неполноценности граждан по признаку их отношения к религии, социальной, расовой, национальной, религиозной или языковой принадлежности; - воспрепятствование законной деятельности органов государственной власти, избирательных комиссий, а также законной деятельности должностных лиц указанных органов, комиссий, соединенное с насилием или угрозой его применения; - публичную клевету в отношении лица, замещающего государственную должность Российской Федерации или государственную должность субъекта Российской Федерации, при исполнении им своих должностных обязанностей или в связи с их исполнением, соединенную с обвинением указанного лица в совершении деяний, указанных в настоящей статье, при условии, что факт клеветы установлен в судебном порядке; - применение насилия в отношении представителя государственной власти либо на угрозу применения насилия в отношении представителя государственной власти или его близких в связи с исполнением им своих должностных обязанностей; - посягательство на жизнь государственного или общественного деятеля, совершенное в целях прекращения его государственной или иной политической деятельности либо из мести за такую деятельность; - нарушение прав и свобод человека и гражданина, причинение вреда здоровью и имуществу граждан в связи с их убеждениями, расовой или национальной принадлежностью, вероисповеданием, социальной принадлежностью или социальным происхождением.
7	Вредоносные программы	программы для ЭВМ, заведомо приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети
8	Преступления	- клевета (распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию); - оскорбление (унижение чести и достоинства другого лица, выраженное в неприлично форме); - публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма; - склонение к потреблению наркотических средств и психотропных веществ; - незаконное распространение или рекламирование порнографических материалов; - публичные призывы к осуществлению экстремистской деятельности; - информация, направленная на пропаганду национальной, классовой, социальной нетерпимости, а также пропаганду социального, расового, национального и религиозного неравенства; - публичные призывы к развязыванию агрессивной войны.
9	Ненадлежащая реклама	информация, содержащая рекламу алкогольной продукции и

№ п/п	Наименование тематической категории	Содержание
		табачных изделий
10	Информация с ограниченным доступом	информация, составляющая государственную, коммерческую, служебную или иную специально охраняемую законом тайну

Типичные угрозы при работе с сетью Интернет и электронной почтой

Угроза	Примечание	Рекомендуемые меры предосторожности
Заражение компьютера вирусом	Чаще всего заражение вирусами происходит при посещении специально созданных «вредоносных» веб-страниц, «хакерских» сайтов, сайтов «для взрослых».	- не посещать перечисленные сайты; - установить, своевременно обновлять и не отключать антивирусное программное обеспечение.
Заражения компьютера вирусом при просмотре почтовых сообщений	Обычно происходит при открытии прикрепленного к письму файла.	- не открывать письма, если электронный адрес отправителя вам не знаком или выглядит «странно»; - не открывать прикрепленные файлы, если отправитель письма вам неизвестен; - установить, своевременно обновлять и не отключать антивирусное программное обеспечение.
Утечка информации с рабочей станции.	Уязвимым может оказаться программное обеспечение (чаще всего таковым является свободно распространяемое ПО, а также ПО от неизвестных или малоизвестных производителей). Также причиной утечки может оказаться заражение компьютера вирусом.	- использовать только принятое к использованию в организации программное обеспечение; - установить, своевременно обновлять и не отключать антивирусное программное обеспечение.
Предоставление возможности удаленного управления компьютером.	Такая возможность может быть получена как с ведома пользователя (при использовании им ПО, выполняющего данную функцию), так и без его ведома (при заражении компьютера вирусом).	- использовать только принятое к использованию в Организации программное обеспечение; - установить, своевременно обновлять и не отключать антивирусное программное обеспечение.
Потеря функциональности (полной или частичной) рабочей станцией	Чаще всего это происходит вследствие использования уязвимостей программного обеспечения злоумышленником или из-за заражения вирусом.	- использовать только принятое к использованию в Организации программное обеспечение; - установить, своевременно обновлять и не отключать антивирусное программное обеспечение.
Кража личной информации.	Чаще всего к этому приводит	- не открывать письма (и особенно

	ввод такой информации на веб-страницах, в том числе сайтах-двойниках, которые внешне идентичны настоящим сайтам(например, сайту банка), но на самом деле являются подделкой	вложения) от незнакомых адресатов; - внимательно проверять адрес страницы, на которой вы собираетесь оставить личную информацию; - не сохранять пароли в формах веб-страниц
Захват адресов электронной почты, веб-страниц и т.п	Чаще всего к этому приводит использование «слабого» пароля для доступа к ресурсу, а также подбор ответа на контрольной вопрос, используемый для восстановления пароля в случае его возможной утери	- использовать «стойкие» пароли (от 7 символов, с использованием букв различного регистра и цифр); - не использовать в качестве ответов на контрольные вопросы (и, конечно, в качестве самих паролей) информацию, которую достаточно легко узнать: дату рождения, имя, фамилию (ваши или близких родственников), кличку собаки, девичью фамилию; - никогда не раскрывать перечисленную выше информацию (если она используется для описанных целей) незнакомым людям; - не сохранять пароли в формах веб-страниц

Общие меры предосторожности при работе с сетью Интернет и электронной почтой

Мера предосторожности	Примечание
Использование только разрешенного отделом информационных технологий и отделом по защите информации программного обеспечения	Использование нерегламентированного ПО может привести к утечке информации, заражению компьютера вирусом, выходу компьютера из строя из-за ошибок в написании ПО. Ответственность возлагается на пользователя
Отслеживание появления обновлений ПО, используемого на компонентах АС организации, взаимодействующих с сетью Интернет	ПО может содержать уязвимости, использование которых злоумышленником может привести к утере информации, выходу компонента из строя. Ответственность возлагается на администраторов соответствующих компонентов
В случае обнаружения в используемом ПО критических с точки зрения безопасности уязвимостей и невозможности их устранения – приостановить эксплуатацию такого ПО	Используемое ПО может содержать уязвимости, использование которых злоумышленником может привести к утере информации, выходу компонента из строя. Ответственность возлагается на пользователей и администраторов соответствующих компонентов АС организации
Обязательное использование и своевременное обновление антивирусного ПО на компонентах АС организации, взаимодействующих с сетью Интернет, в режиме мониторинга событий	Заражение вирусами может произойти и без «интерактивного» участия пользователя – достаточно связи с сетью Интернет. Ответственность возлагается на администраторов соответствующих компонентов.
При работе с электронной почтой – не	В последнее время наиболее распространенный канал

открывать письма с вложенными файлами от неизвестных авторов, перед запуском/открытием любых файлов производить их антивирусную проверку	распространения вирусов, а также кражи личной информации – электронная почта. В случае возникновения вопросов необходимо обратиться в отдел по защите информации до принятия решения о дальнейших действиях. Ответственность возлагается на пользователей
Запретить автоматическое сохранение и/или запуск файлов и элементов ActiveX, скриптов из сети Интернет на рабочей станции пользователя	Большинство уязвимостей в программном обеспечении используются через файлы, загружаемые с веб-страниц, или через сами веб-страницы, которые содержат вредоносный/опасный код. Для опытных пользователей с разрешения отдела по защите информации допускается возможность предоставления выбора о необходимости загрузки/запуска таких элементов. Ответственность возлагается на пользователей
Не рекомендуется сохранять пароли в формах при посещении веб-страниц	Это может привести к тому, что кто-то иной воспользуется (в то числе – изменит пароль на новый) ресурсом, защищенным паролем. Ответственность возлагается на пользователей