Муниципальное общеобразовательное учреждение
«Средняя общеобразовательная Учреждение №4» г. Всеволожска
(МОУ СОШ №4 г.Всеволожска)

ПРИНЯТО
Педагогическим советом
МОУ СОШ № 4 г. Всеволожска
протокол от «28» августа 2020 г. № 01

УТВЕРЖДЕНО
Приказом МОУ СОШ №4 г. Всеволожска
От 28 августа 2020 г. № 149-ОД

Правила использования сети «Интернет» в МОУ СОШ №4 г. Всеволожска

1. Общие положения

Правила использования сети Интернет в МОУ СОШ №4 г. Всеволожска (далее Правила) разработаны в соответствии с Конституцией РФ, Федеральным законом Российской Федерации от 29.12.2012 г. №273-ФЗ «Об образовании в Российской Федерации», Федеральным законом от 29.12.2010 г. № 436-ФЗ (ред. 31.07.2020) «О защите детей от информации, причиняющей вред их здоровью и развитию», Уставом МОУ СОШ №4 г.Всеволожска (далее – ОУ).

2. Общие правила

2.1. При использовании сети Интернет в ОУ обучающимся и учителям (далее – пользователи) предоставляется доступ только к тем ресурсам, содержание которых не противоречит законодательству Российской Федерации, и которые имеют прямое отношение к образовательному процессу. Проверка выполнения такого требования осуществляется с помощью специальных технических средств и программного обеспечения контентной фильтрации, установленного в ОУ на компьютерах с неограниченным доступом для обучающихся или предоставленного оператором услуг связи.

2.2 Во время уроков и других занятий в рамках учебного процесса контроль использования обучающимися сети Интернет осуществляет преподаватель, ведущий занятие. При этом преподаватель: - наблюдает за использованием компьютера в сети Интернет обучающимися; - принимает меры по пресечению обращений к ресурсам, не имеющим отношения к образовательному процессу.

2.3.Во время свободного доступа обучающихся к сети Интернет вне учебных занятий, контроль использования ресурсов Интернета осуществляют работники школы, в чьих кабинетах находятся компьютеры - наблюдают за использованием компьютера в сети Интернет обучающимися; - принимают меры по пресечению обращений к ресурсам, не имеющим отношения к образовательному процессу.

3. Особые ситуации

Пользователи сети Интернет в ОУ должны учитывать, что технические средства и программное обеспечение не могут обеспечить полную фильтрацию ресурсов сети Интернет вследствие частого обновления ресурсов. В связи с этим существует вероятность обнаружения обучающимися ресурсов, не имеющих отношения к образовательному процессу, содержание которых противоречит законодательству Российской Федерации. Участникам использования сети Интернет в ОУ следует осознавать, что ОУ не несет ответственности за случайный доступ к подобной информации, размещенной не на Интернет-ресурсах образовательной организации. При

обнаружении указанной информации пользователю необходимо сообщить об этом ответственному за использование сети Интернет в ОУ, указав при этом адрес ресурса.

4. **Для дополнительной защиты в МОУ СОШ №4 г. Всеволожска используется лицензионное антивирусное программное обеспечение.**

4.1. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

4.2. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

4.3. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов.

4.4. Ежедневно в начале работы при загрузке компьютера (для серверов ЛВС - при перезапуске) в автоматическом режиме должно выполняться обновление антивирусных баз и проводиться антивирусный контроль всех дисков и файлов персонального компьютера.

4.5. Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера должен выполняться: Непосредственно после установки (изменения) программного обеспечения компьютера (локальной вычислительной сети), должна быть выполнена антивирусная проверка: на серверах и персональных компьютерах образовательного учреждения. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.).

4.6. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователи обязаны: приостановить работу; немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение информационной безопасности в образовательном учреждении; совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования; провести лечение или уничтожение зараженных файлов; в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, ответственный за антивирусную защиту обязан направить зараженный вирусом файл на внешнем носителе в организацию, с которой заключен договор на антивирусную поддержку для дальнейшего исследования.

5. **Права, обязанности и ответственность пользователей**

5.1. Пользователи имеют право:

5.1.1. Работать в сети Интернет

5.1.2. Сохранять полученную информацию на съемном накопителе.

5.2. Пользователям запрещается:

5.2.1. Осуществлять действия, запрещенные законодательством РФ.

5.2.2. Посещать сайты, содержание и тематика которых не допустимы для несовершеннолетних и/или нарушают законодательство Российской Федерации (порнография, эротика, пропаганда насилия, терроризма, политического и религиозного экстремизма, национальной, расовой и т.п. розни, иные ресурсы схожей направленности).

5.2.3.Загрузка и распространение материалов, содержащих вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или

телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в Интернете, а также размещения ссылок на вышеуказанную информацию.

5.2.4. Загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным пакетом.

5.2.5 .Передавать информацию, представляющую коммерческую или государственную тайну, распространять информацию, порочащую честь и достоинство граждан.

5.2.6. Устанавливать на компьютерах дополнительное программное обеспечение, как полученное в Интернете, так и любое другое без специального разрешения.

5.2.7. Изменять конфигурацию компьютеров, в том числе менять системные настройки компьютера и всех программ, установленных на нем.

5.2.8.Осуществлять действия, направленные на "взлом" любых компьютеров, находящихся как в «точке доступа к Интернету» ОУ, так и за его пределами.

5.2.9. Использовать возможности «точки доступа к Интернету» ОУ для пересылки и записи непристойной, клеветнической, оскорбительной, угрожающей и порнографической продукции, материалов и информации.

5.2.10. Осуществлять любые сделки через Интернет.

5.3. Пользователи несут ответственность:

5.3.1. За содержание передаваемой, принимаемой и печатаемой информации.

5.3.2. За нанесение любого ущерба оборудованию в «точке доступа к Интернету» (порча имущества, вывод оборудования из рабочего состояния) пользователь несет материальную ответственность.

5.3.3. При случайном обнаружении ресурса, содержание которого не имеет отношения к образовательному процессу, следует незамедлительно сообщить об этом преподавателю, проводящему занятие. Преподаватель обязан зафиксировать доменный адрес ресурса, время его обнаружения и сообщить об этом лицу, ответственному за работу сети и ограничение доступа к информационным ресурсам с тем, чтобы этот ресурс был занесен в общий список запрещенных ресурсов.