

Комитет по образованию администрации муниципального образования  
«Всеволожский муниципальный район» Ленинградской области  
**МУНИЦИПАЛЬНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ БЮДЖЕТНОЕ  
УЧРЕЖДЕНИЕ  
«СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА  
«МУРИНСКИЙ ЦЕНТР ОБРАЗОВАНИЯ № 2»  
(МОБУ «СОШ «МУРИНСКИЙ ЦО № 2»)**

**ПРИНЯТО**

Педагогическим советом  
МОБУ «СОШ «Муринский ЦО № 2»  
(протокол № 4 от 25 марта 2021 г.)

**УТВЕРЖДЕНО**

приказом МОБУ «СОШ «Муринский ЦО № 2»  
от 02 апреля 2021 г. № 149-о

**ПОЛОЖЕНИЕ  
об использовании сети Интернет в МОБУ «СОШ «Муринский ЦО №2»**

г. Мурино  
2021 г.

## 1. Общие положения

Правила использования сети Интернет в МОБУ «СОШ «Муринский ЦО №2» (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 школы.

## 2. Общие правила

2.1. При использовании сети Интернет в ОУ учащимся 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 школе 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 школе 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 школа 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 школе, указав при этом адрес ресурса.

4. Для дополнительной защиты в МОБУ «СОШ «Муринский ЦО №2» 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

Пользователи имеют право:

### 5.1. Работать в сети Интернет

### 5.2. Сохранять полученную информацию на съемном накопителе.

Пользователям запрещается:

- 5.3. Осуществлять действия, запрещенные законодательством РФ.
- 5.4. 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).
- 5.5. 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.
- 5.6. Загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным пакетом.
- 5.7. Передавать информацию, представляющую коммерческую или государственную тайну, распространять информацию, порочащую честь и достоинство граждан.
- 5.8. Устанавливать на компьютерах дополнительное программное обеспечение, как полученное в Интернете, так и любое другое без специального разрешения.
- 5.9. Изменять конфигурацию компьютеров, в том числе менять системные настройки компьютера и всех программ, установленных на нем.
- 5.10. Осуществлять действия, направленные на "взлом" любых компьютеров, находящихся как в «точке доступа к Интернету» ОУ, так и за его пределами.
- 5.11. Использовать возможности «точки доступа к Интернету» ОУ для пересылки и записи непристойной, клеветнической, оскорбительной, угрожающей и порнографической продукции, материалов и информации.
- 5.12. Осуществлять любые сделки через Интернет.

Пользователи несут ответственность:

- 5.13. За содержание передаваемой, принимаемой и печатаемой информации.
- 5.14. За нанесение любого ущерба оборудованию в «точке доступа к Интернету» (порча имущества, вывод оборудования из рабочего состояния) пользователь несет материальную ответственность.
- 5.15. 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.

Подписано цифровой  
подписью: МОБУ «СОШ  
«МУРИНСКИЙ ЦО №2»