

ПРИНЯТО
Общим собранием работников
МБУ ДО «Станция юных
натуралистов»
Протокол от 16.08.2021 года №7

УТВЕРЖДАЮ
Директор МБУ ДО «Станция
юных натуралистов»

Н.Н. Литвинова
Приказ от 16.08.2021 года №159

**Регламент доступа учащихся
муниципального бюджетного учреждения дополнительного образования
«Станция юных натуралистов» Красногвардейского района
Белгородской области к точкам подключения на территории
учреждения к сети Интернет**

1. Общие положения

1.1. Использование сети Интернет в муниципальном бюджетном учреждении дополнительного образования «Станция юных натуралистов» Красногвардейского района Белгородской области (далее - учреждение) направлено на решение задач учебно-воспитательного процесса.

1.2. Настоящий регламент регулирует условия и порядок использования сети Интернет в учреждении.

2. Организация использования сети Интернет в учреждении

2.1. Настоящий Регламент регулирует условия и порядок использования сети Интернет в учреждении.

2.2. Во время занятий контроль использования учащимися сети Интернет осуществляет педагог дополнительного образования: наблюдает за использованием компьютера в сети Интернет учащимися; принимает меры по пресечению обращений к ресурсам, не имеющим отношения к образовательному процессу; дает разрешение и контролирует процесс скачивания информации из сети Интернет.

2.3. Во время свободного доступа учащихся, педагогов к сети Интернет вне учебных занятий, контроль использования ресурсов Интернета осуществляет педагог, методист, присутствующий в кабинете вместе с учащимся и посредством ведения журнала учета работы конкретного пользователя на конкретном месте (ФИО пользователя, объединение, дата, время — с ... до ...). Помимо этого на сервере контентной фильтрации ведется учет посещений учащимися и педагогами интернет-ресурсов, включающий механизм идентификации по логину и паролю. Ответственный за информационную безопасность учреждения посредством анализа журналов (логов) на сервере контентной фильтрации и анализа истории браузера (при необходимости) может в случае выявления попыток нарушения контентной фильтрации:

- принять меры по пресечению обращений к ресурсам, не имеющим отношения к образовательному процессу (закрывать доступ);
- контролировать объем скачиваемой информации;
- удалить учетную запись идентифицирующую пользователя на сервере с целью пресечения не санкционируемого доступа пользователя.

2.4. При использовании сети Интернет в учреждении учащимся предоставляется доступ только к тем ресурсам, содержание которых не противоречит законодательству Российской Федерации и которые имеют отношение к образовательному процессу.

2.5. Отнесение определенных ресурсов и (или) категорий ресурсов в соответствующие группы, доступ к которым регулируется техническими средствами и программным обеспечением контентной фильтрации, обеспечивается ответственным за функционирование средств контент-фильтрации.

3. Права, обязанности и ответственность пользователей

3.1. Использование сети Интернет в учреждении осуществляется в целях образовательного процесса.

3.2. Педагоги и учащиеся могут пользоваться доступом к глобальным Интернет-ресурсам по разрешению директора и/или лица, назначенного ответственным за функционирование средств контент-фильтрации.

3.3. К работе в сети Интернет допускаются лица прошедшие инструктаж и обязавшиеся соблюдать Регламент работы.

3.4. Пользователям запрещается:

3.4.1. Осуществлять действия, запрещенные законодательством РФ.

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

3.4.3. Загружать и распространять материалы, содержащие 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.

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

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

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

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

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

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

3.4.10. Осуществлять любые не законные сделки через Интернет.

3.5. Пользователи несут ответственность:

3.5.1. За содержание передаваемой, принимаемой и печатаемой информации.

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

3.6. Педагоги имеют право:

3.6.1. Работать в сети Интернет в течение периода времени, определенного директором и/или ответственным за функционирование средств контент-фильтрации учреждения.

3.6.2. Сохранять полученную информацию на съемном диске, файловом сервере, облачном хранилище.

4. Общие положения

4.1. Данное положение принимается на общем собрании работников учреждения и утверждается приказом директора по учреждению.

4.2. Данное положение размещается на официальном сайте учреждения в разделе «Информационная безопасность».