

Состав

Совета по вопросам регламентации доступа к информации в сети Интернет
при МОБУ «Кисельнинская средняя школа»

Председатель Совета:

-Степанюк А.В.-зам. директора школы по безопасности

Заместитель председателя:

-Дунаева В.В.-зам. директора школы по УВР

Члены Совета:

-Михайлов Павел -ученик 9 класса

-Маркова Н.М.- председатель Совета родителей

-Куприянова М.С.- учитель

Приложение 2
к приказу директора школы
№ 119/1 от 29.08.2014

Принято С учетом мнения Совета учреждения Протокол от 28.08.2014 г.	
---	--

Положение о Совете по вопросам регламентации доступа к информации в сети Интернет при МОБУ «Кисельнинская средняя школа»

1. В соответствии с настоящим Положением о Совете по вопросам регламентации доступа к информации в Интернете (далее — Совет) целью создания Совета является принятие мер по ограничению доступа обучающихся к ресурсам сети Интернет, содержащим информацию, не имеющую отношения к образовательному процессу.
2. Совет осуществляет непосредственное определение политики доступа в Интернет.
3. Совет создается из представителей педагогического коллектива, Совета родителей и Совета учащихся в согласованном порядке.
4. Очередные собрания Совета проводятся с периодичностью, установленной Советом.
5. Совет:
 - принимает решения на основе методических рекомендаций и классификационных списков ресурсов о разрешении/блокировании доступа к определенным ресурсам и (или) категориям ресурсов сети Интернет, содержащим информацию, не имеющую отношения к образовательному процессу, с учетом социокультурных особенностей конкретного региона, мнения членов Совета, а также иных заинтересованных лиц, представивших свои предложения в Совет;
 - определяет характер и объем информации, публикуемой на сайте школы;
 - направляет директору школы рекомендации о назначении и освобождении от исполнения своих функций сотрудников, ответственных за непосредственный контроль безопасности работы обучающихся в сети Интернет и ее соответствия целям и задачам образовательного процесса.
6. Принятие решений о политике доступа к ресурсам/группам ресурсов сети Интернет осуществляется Советом самостоятельно и возможно с привлечением внешних экспертов:
 - преподавателей образовательного учреждения и других образовательных учреждений;
 - специалистов в области информационных технологий и обеспечения безопасного доступа;
 - представителей органов управления образованием.
7. При принятии решений Совет должен руководствоваться:
 - законодательством Российской Федерации;
 - специальными познаниями, в том числе полученными в результате профессиональной деятельности по рассматриваемой тематике;
 - интересами обучающихся, целями образовательного процесса;
 - рекомендациями профильных органов и организаций в сфере классификации ресурсов сети Интернет.
8. Отнесение определенных категорий и/или ресурсов к соответствующим группам, доступ к которым регулируется техническими средствами и программным обеспечением ограничения доступа к информации, осуществляется на основании решений Совета лицом, директором школы по представлению Совета.
9. Категории ресурсов, в соответствии с которыми определяется политика использования сети Интернет в образовательном учреждении, доступ к которым регулируется техническими

средствами и программным обеспечением технического ограничения доступа к информации, определяются в установленном порядке.

Приложение 3
к приказу директора школы
№ 119/1 от 29.08.2014

Инструкцию по осуществлению мониторинга эффективности работы СКФ в МОБУ «Кисельнинская средняя школа»

1. Общие требования:

1. Проверяемое автоматизированное рабочее место (далее – АРМ) должно иметь доступ к сети Интернет и использоваться обучающимися школы.
2. По согласованию на период контрольных мероприятий, может быть приглашен специалист ОАО «ОНЛАЙН».
3. При проведении проверки необходимо обеспечить присутствие представителя школы (директор школы, заместитель директора школы, сотрудник, ответственный за доступ к сети Интернет в ОУ).

Мероприятия при общем мониторинге:

1. Выбрать 3-4 материала, содержание которых может причинить вред здоровью и развитию обучающихся (Федеральный список экстремистских материалов - <http://minjust.ru/nko/fedspisok>). Проверить конкретный сайт можно в едином реестре доменных имен, указателей страниц сайтов в сети Интернет и сетевых адресов, позволяющих идентифицировать сайты в сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено - <http://zapret-info.gov.ru/>, <http://eais.rkn.gov.ru/>.
2. Внести название материала (части материала, адрес сайта) в поисковую систему.
3. Из предложенного поисковой системой списка адресов перейти на страницу сайта, содержащего противоправный контент. Если материал отображается и с ним можно ознакомиться без дополнительных условий – фиксируется факт нарушения работы системы контентной фильтрации.
4. При дополнительных условиях (требуется регистрация, условное скачивание, переадресация и т.д.), при выполнении которых материал отображается, также фиксируется факт нарушения работы системы контентной фильтрации. При невозможности ознакомления с противоправным контентом при выполнении условий (регистрация, скачивание материалов, переадресаций и т.д.) нарушение не фиксируется.

Мероприятия при тематическом мониторинге (при необходимости):

1. Выбрать 3-4 противоправных материала по определенной теме (экстремизм, проявление жестокости, порнография, терроризм, суицид, насилие и т.д.).
2. Запросить через поисковую систему материал по заданной теме (Например: «изготовление зажигательной бомбы», «способы суицида» и т.д.).
3. Из предложенного поисковой системой списка адресов перейти на страницу 2-3 сайтов и ознакомиться с полученными материалами.
4. Дать оценку материалам на предмет возможного нанесения ущерба физическому и психическому здоровью обучающихся.
5. При признании материала условно противоправным – зафиксировать факт нарушения с указанием источника и мотивов оценки, а также направить адрес материала на проверку в единый реестр доменных имен, указателей страниц сайтов в сети Интернет и сетевых адресов, позволяющих идентифицировать сайты в сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено - <http://zapret-info.gov.ru/>, <http://eais.rkn.gov.ru/>.

По итогам мониторинга сформировать заключение (отчет) об эффективной (неэффективной) работе контентной фильтрации. При неэффективной работе контент-фильтра, в заключении необходимо указать выявленные проблемы, пути их решения и сроки исправления.

Отчет о проведении мониторинга эффективности использования систем контентной фильтрации в образовательной организации

1. Характеристика систем контентной фильтрации в образовательной организации

№ п/п	Критерий	Значение критерия		
		ОО	ДОО	ОДО
1.1.	Способ осуществления контент-фильтрации для обучающихся:			
1.1.1.	осуществляется провайдером			
1.1.2.	осуществляется программными средствами			
1.1.3.	осуществляется аппаратными средствами			
1.2.	Принцип работы контент-фильтра для обучающихся			
1.2.1.	белые списки			
1.2.2.	черные списки			

№ п/п	Критерий	Значение критерия		
		ОО	ДОО	ОДО
1.	Наличие контент-фильтра для администрации образовательной организации			

2. Тестирование эффективности настройки программных средств, осуществляющих контентную фильтрацию в образовательной организации

№ п/п	Критерий	Значение критерия
2.1.	Проверка эффективности настройки СКФ на доступность сайтов экстремистской направленности	
2.1.1.	Результат проверки по запросу списка ресурсов	
2.1.2.	Результат проверки по запросу картинок	
2.1.3.	Результат проверки ресурсов по URL-адресу	
2.2.	Проверка эффективности настройки СКФ на доступность сайтов порнографического характера	
2.2.1.	Результат проверки по запросу списка ресурсов	
2.2.2.	Результат проверки по запросу картинок	
2.2.3.	Результат проверки ресурсов по URL-адресу	
2.3.	Проверка эффективности настройки СКФ на доступность сайтов, содержащих информацию об алкогольной продукции, изготовлении и использовании наркотических средств, психотропных веществ, способах совершения самоубийства	
2.3.1.	Результат проверки по запросу списка ресурсов	
2.3.2.	Результат проверки по запросу картинок	
2.3.3.	Результат проверки ресурсов по URL-адресу	
2.4.	Определение эффективности использования систем контентной фильтрации	
2.4.1.	Оценка эффективности работы СКФ в образовательной организации (указывается в % среднее значение по п.п. 2.1.1.-2.1.3, 2.2.1.-2.2.3, 2.3.1.-2.3.3)	

Регламент организации доступа к сети Интернет

1. Общие положения

Настоящий регламент разработан в связи с широким применением информационных ресурсов сети Интернет в образовательном процессе во исполнении требований Федерального закона от 29.12.2010 №436-ФЗ (ред. от 02.07.2013) «О защите детей от информации, причиняющей вред их здоровью и развитию» в целях исключения доступа обучающихся образовательных учреждений к ресурсам сети Интернет, содержащим информацию, несовместимую с задачами образования и воспитания учащихся, в соответствии с Федеральным законом «Об образовании в Российской Федерации» от 29 декабря 2012 г. №273-ФЗ.

Использование сети Интернет в образовательном учреждении МОБУ «Бережковская основная общеобразовательная школа» должно быть направлено на решение задач учебно-воспитательного процесса. При организации доступа в сеть учителя сталкиваются с проблемами технического, организационного и педагогического характера. Регламент определяет порядок эффективного использования сети Интернет, ограничение доступа к ресурсам сети, не имеющим отношения к образовательному процессу, а также время работы в сети.

Выход в сеть должен быть обусловлен поставленной целью, так например: поиск информации; усиление мотивации в изучении учащимися образовательных дисциплин; подготовка к государственной итоговой аттестации; тестирование; участие в Интернет-олимпиадах, конкурсах; подготовка к поступлению в учреждения профессионального образования; погружение в языковую среду; проведение исследовательской работы; дистанционное обучение и использование его элементов в образовательном процессе; повышение квалификации педагогов; отработка навыков, развитие коммуникационного (сетевое) общения; опубликование интересных авторских материалов педагогов и учащихся, обмен опытом; создание веб-страниц; создание мультимедиа презентаций; электронная отчетность; другое.

К работе в сети Интернет допускаются участники образовательного процесса, прошедшие предварительную регистрацию у лица, ответственного за доступ к сети по образовательному учреждению.

Настоящий Регламент регулирует условия и порядок использования сети Интернет в МОБУ «Кисельнинская средняя школа» .

2. Организация использования сети Интернет

2.1. Вопросы использования возможностей сети Интернет в учебно-образовательном процессе рассматриваются на педагогическом совете школы.

2.2. Регламентация доступа к информации сети Интернет определяется педагогическим советом на основании предложений педагогов о закрытии определенных сайтов.

2.3. Педагогический совет утверждает Правила использования сети Интернет на учебный год. Правила вводятся в действие приказом директора школы.

Правила использования сети Интернет разрабатываются педагогическим советом школы на основе настоящего регламента самостоятельно.

При разработке правил использования сети Интернет педагогический совет руководствуется:

- законодательством Российской Федерации;
- опытом целесообразной и эффективной организации учебного процесса с использованием информационных технологий и возможностей Интернета;
- интересами обучающихся;
- целями образовательного процесса;

2.4. Педагогический совет школы:

- принимает решение о блокировании доступа к определенным ресурсам и (или) категориям ресурсов сети Интернет;
- определяет характер и объем информации, публикуемой на Интернет-ресурсах школы;
- дает рекомендации о назначении и освобождении от исполнения своих функций лиц, ответственных за обеспечение доступа к ресурсам сети Интернет и контроль безопасности работы в Сети.

2.5. Директор школы отвечает за обеспечение эффективного и безопасного доступа к сети Интернет в ОУ, а также за выполнение установленных правил.

2.6. Для обеспечения доступа участников образовательного процесса к сети Интернет, в соответствии с установленными в ОУ правилами, директор школы назначает своим приказом ответственного за организацию работы с сетью Интернет и контроль безопасности работы в сети, а также вносит изменения в должностные инструкции работников, использующих ресурсы сети в образовательном процессе, в соответствии с рекомендациями.

2.7. Во время уроков и других занятий в рамках образовательного процесса, а также во время свободного доступа обучающихся к сети Интернет вне учебных занятий контроль использования обучающимися информационной сети осуществляет преподаватель, ведущий занятие, или работники школы, определенные приказом его руководителя.

Учитель информатики и ИКТ:

- организует работу в сети;
- наблюдает за использованием компьютеров и сети Интернет обучающимися;
- принимает меры по пресечению обращений к ресурсам, не имеющим отношения к образовательному процессу;
- ведет записи в регистрационном журнале доступа к сети Интернет;
- сообщает классному руководителю о преднамеренных попытках обучающегося осуществить обращение к ресурсам, не имеющим отношения к образовательному процессу;
- в целях экономии трафика создает и ведет накопительную базу образовательных Интернет-ресурсов.

2.8. При использовании сети Интернет участникам образовательного процесса предоставляется доступ только к тем ресурсам, содержание которых не противоречит законодательству Российской Федерации и которые имеют прямое отношение к образовательному процессу. Ограничение доступа к ресурсам сети, несовместимым с задачами обучения и воспитания, осуществляется с помощью установки на компьютерах (сервере) специальных программ, запрещающих доступ к определенным сайтам, или использованием технических и программных средств контентной фильтрации, установленных в школе или предоставленных оператором услуг связи.

2.9. В связи с невозможностью техническими и программными средствами добиться полной фильтрации ресурсов сети Интернет вследствие их частого обновления, необходимо присутствие педагога или другого ответственного лица при работе обучающихся в сети.

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

В случае обнаружения ресурса, несовместимого с задачами обучения и воспитания несовершеннолетних, и/или нарушающего законодательство Российской Федерации (эротика, порнография, пропаганда насилия, терроризма, политического или религиозного экстремизма, национальной, расовой и т. п. розни, иные ресурсы схожей направленности), ответственный за организацию работы с сетью Интернет и контроль безопасности работы в сети должен незамедлительно, без согласования с педагогическим или специальным советом закрыть доступ к данному источнику.

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

- соблюдение действующего законодательства Российской Федерации, интересов и прав граждан;
- защиту персональных данных обучающихся, преподавателей и сотрудников;

- 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, только с письменного согласия родителей или иных законных представителей обучающихся. Персональные данные преподавателей и сотрудников школы размещаются на его Интернет-ресурсах только с письменного согласия лица, чьи персональные данные размещаются.

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.

2.14. При получении согласия на размещение персональных данных представитель школы обязан разъяснить возможные риски и последствия их опубликования. Школа не несет ответственности за такие последствия, если предварительно было получено письменное согласие лица (его законного представителя) на опубликование персональных данных.

3. Использование сети Интернет в образовательном учреждении

3.1. Использование сети Интернет в школе осуществляется, как правило, в целях образовательного процесса.

3.2. По разрешению лица, ответственного за организацию в школе работы сети Интернет и ограничение доступа, преподаватели, сотрудники и обучающиеся вправе размещать собственную информацию в сети Интернет на Интернет-ресурсах школы и иметь учетную запись электронной почты.

3.3. Работникам школы и обучающимся запрещается:

- обращаться к ресурсам, содержание и тематика которых не допустимы для несовершеннолетних и/или нарушают законодательство Российской Федерации;
- осуществлять любые сделки через Интернет;
- использовать сеть Интернет в коммерческих целях;
- 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 образовательному процессу, обучающийся обязан незамедлительно сообщить об этом преподавателю, проводящему занятие. Преподаватель должен зафиксировать доменный адрес ресурса и сообщить об этом лицу, ответственному за работу в сети Интернет.

Ответственный обязан:

- принять информацию от преподавателя и, в случае наличия технической возможности, внести указанный ресурс в число запрещенных, или направить информацию о некатегоризированном ресурсе оператору технических средств и программного и технического ограничения доступа к информации.

Регламент работы с электронной почтой

1. Общие положения

1.1. МОБУ «Кисельнинская средняя школа» имеет свой адрес электронной почты: kiseln.school@mail.ru

1.2. Электронная почта в школе (далее - ОУ) может использоваться только в административных и образовательных целях. Пользователи и владельцы электронных почтовых ящиков должны соблюдать правила и инструкции по работе с электронной почтой, этические нормы общения.

1.3. Перед отправлением сообщения или отчета необходимо проверить правописание и грамматику текста.

1.4. Пользователям данного сервиса запрещено:

- участвовать в рассылке посланий, не связанных с образовательной или административной деятельностью Учреждения;
- пересылать по произвольным адресам не затребованную потребителями информацию (спам);
- отправлять сообщения противозаконного или неэтичного содержания;
- использовать массовую рассылку электронной почты, за исключением необходимых случаев;
- электронное послание не должно использоваться для пересылки секретной и конфиденциальной информации, регламент обмена которыми утверждается иными нормативно-правовыми актами.

2. Порядок обработки, передачи и приема документов по электронной почте

2.1. По электронной почте производится получение и отправка информации законодательного, нормативно-правового, учебного, учебно-методического характера, а также любой другой информации, совместимой с процессом образования.

2.2. Для обработки, передачи и приема информации по электронной почте в ОУ приказом директора назначается ответственное лицо – оператор электронной почты.

2.3. Ответственность за ненадлежащую подготовку информации к передаче по электронной почте несет автор информации, предполагаемой к отправке; ответственность за отправку адресату и получение электронной почты – несет оператор электронной почты.

2.4. Размер вложения почтового сообщения не должен превышать 50 Мбайт.

2.5. Все передаваемые учебно-методические и справочно-информационные материалы должны передаваться с сопроводительным письмом. Для отправки электронного сообщения пользователь оформляет документ в соответствии с требованиями по делопроизводству, утвержденными в образовательном учреждении.

2.6. При получении электронного сообщения оператор:

- передает документ на рассмотрение администрации ОУ или в случае именного сообщения - непосредственно адресату;
- в случае невозможности прочтения электронного сообщения уведомляет об этом отправителя.

2.7. При оформлении электронного сообщения обязательны к заполнению следующие поля:

- адрес получателя;
- тема электронного сообщения;
- текст электронного сообщения (при необходимости, могут быть вложены файлы);
- подпись отправителя с указанием наименования ОУ и его структурного подразделения, сотрудником которого является отправитель.

2.8. Отправка и получение электронных документов осуществляется с использованием программных продуктов, предназначенных для работы с электронной почтой в ОУ.

3. Ответственность

3.1. Изменение наименования официального ЭПЯ ОУ согласовывает со специалистами Комитета по образованию Волховского муниципального района, ведущими электронный документооборот и отвечающими за информатизацию системы муниципального образования.

3.2. По факту изменения официального ЭПЯ ОУ обязано уведомить информационным письмом Комитет по образованию за 3 рабочих дня до смены ЭПЯ с указанием даты, с которой изменения вступают в силу.

3.3. Ответственность за функционирование электронного документооборота в учреждении несет директор школы.

Регламент организации антивирусной защиты

1. Общие положения

Целью создания системы антивирусной защиты является обеспечение защищенности информационно-коммуникационной системы (далее ИКС) от воздействия различного рода вредоносных программ и несанкционированных массовых почтовых рассылок, предотвращения их внедрения в информационные системы, выявления и безопасного удаления из систем в случае попадания, а также фильтрации доступа пользователей МОБУ «Кисельнинская средняя школа» (далее по тексту - ОУ) к непродуктивным Интернет-ресурсам и контроля их электронной переписки.

Основополагающими требованиями к системе антивирусной защиты ОУ являются:

- решение задачи антивирусной защиты должно осуществляться в общем виде. Средство защиты не должно оказывать противодействие конкретному вирусу или группе вирусов, противодействие должно оказываться в предположениях, что вирус может быть занесен на компьютер и о вирусе (о его структуре (в частности, сигнатуре) и возможных действиях) ничего не известно;

- решение задачи антивирусной защиты должно осуществляться в реальном времени.

2. Мероприятия, направленные на решение задач по антивирусной защите:

- установка только лицензированного программного обеспечения.

- регулярное обновление и ежедневные профилактические проверки (желательно в нерабочее ночное время);

- непрерывный контроль над всеми возможными путями проникновения вредоносных программ, мониторинг антивирусной безопасности и обнаружение деструктивной активности вредоносных программ на всех объектах ИКС;

- ежедневный анализ, ранжирование и предотвращение угроз распространения и воздействия вредоносных программ путем выявления уязвимостей используемого в ИКС операционного программного обеспечения и сетевых устройств и устранения обнаруженных дефектов в соответствии с данными поставщика программного обеспечения и других специализированных экспертных антивирусных служб.

- проведение профилактических мероприятий по предотвращению и ограничению вирусных эпидемий, включающих загрузку и развертывание специальных правил нейтрализации (отражению, изоляции и ликвидации) вредоносных программ на основе рекомендаций по контролю атак, подготавливаемых разработчиком средств защиты от вредоносных программ и другими специализированными экспертными антивирусными службами до того, как будут выпущены файлы исправлений, признаков и антивирусных сигнатур.

- проведение регулярных проверок целостности критически важных программ и данных. Наличие лишних файлов и следов несанкционированного внесения изменений должно быть зарегистрировано в журнале и расследовано;

- внешние носители информации неизвестного происхождения следует проверять на наличие вирусов до их использования;

- необходимо строго придерживаться установленных процедур по уведомлению о случаях поражения автоматизированной информационной среды компьютерными вирусами и принятию мер по ликвидации последствий от их проникновения;

- следует иметь планы обеспечения бесперебойной работы ОУ для случаев вирусного заражения, в том числе планы резервного копирования всех необходимых данных и программ и их восстановления. Эти меры особенно важны для сетевых файловых серверов, поддерживающих большое количество рабочих станций.

3. Технологические инструкции

Директором школы должно быть назначено лицо, ответственное за антивирусную защиту, в

должностные инструкции для которого должны быть прописаны порядок действия в период вирусных эпидемий, порядок действий при возникновении внештатных ситуаций, связанных с работоспособностью средств антивирусной защиты, порядок действий для устранения последствий заражений. В противном случае вся ответственность за обеспечение антивирусной защиты ложится на директора школы.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы, почтовые сообщения), получаемая и передаваемая по телекоммуникационным каналам связи, а также информация, находящаяся на съемных носителях (магнитных дисках, лентах, CD-ROM, DVD, flash-накопителях и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

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

2. Требования к проведению мероприятий по антивирусной защите

2.1. В начале работы при загрузке компьютера в автоматическом режиме должно выполняться обновление антивирусных баз и серверов.

2.2. Периодические проверки электронных архивов должны проводиться не реже одного раза в неделю, данные, расположенные на рабочих станциях пользователей – ежедневно, в ночное время по расписанию.

2.3. Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера должен выполняться:

2.3.1. Непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка на серверах и персональных компьютерах учреждения.

2.3.2. 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.).

2.3.3. При отправке и получении электронной почты оператор электронной почты обязан проверить электронные письма и их вложения на наличие вирусов.

2.4. В случае обнаружения зараженных вирусами файлов или электронных писем пользователи обязаны:

2.4.1. Приостановить работу.

2.4.2. Немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение антивирусной защиты (в случае его отсутствия – директора ОУ).

2.4.3. Совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования.

2.4.4. Провести лечение или уничтожение зараженных файлов.

3. Ответственность

3.1. Ответственность за организацию антивирусной защиты возлагается на директора школы или лицо, им назначенное.

3.2. Ответственность за проведение мероприятий антивирусного контроля в ОУ возлагается на ответственного за обеспечение антивирусной защиты, соблюдение требований настоящей Инструкции при работе на персональных рабочих станциях возлагается на пользователей данных станций или педагога, отвечающего за работу компьютерного класса.

3.3. Периодический контроль за состоянием антивирусной защиты в ОУ осуществляется директором школы и фиксируется Актом проверки (не реже 1 раза в квартал).

**Инструкция для сотрудников о порядке действий
при осуществлении контроля использования обучающимися сети Интернет**

1. Настоящая инструкция устанавливает порядок действий сотрудников МОБУ «Кисельнинская средняя школа» (далее по тексту -ОУ) при обнаружении:

- 1) обращения обучающихся к контенту, не имеющему отношения к образовательному процессу;
- 2) отказа при обращении к контенту, имеющему отношение к образовательному процессу, вызванного техническими причинами.

2. Контроль использования обучающимися сети Интернет осуществляют:

- 1) во время занятия — проводящий его преподаватель;
- 2) во время использования сети Интернет для свободной работы обучающихся — работник школы, назначенный директором ОУ в установленном порядке.

3. Учитель или работник школы, назначенный директором ОУ в установленном порядке:

— определяет время и место работы обучающихся в сети Интернет с учетом использования в образовательном процессе соответствующих технических возможностей, а также длительность сеанса работы одного обучающегося;

— наблюдает за использованием обучающимися компьютеров и сети Интернет;

— способствует осуществлению контроля объемов трафика ОУ в сети Интернет;

— запрещает дальнейшую работу обучающегося в сети Интернет на уроке (занятии) в случае нарушения им порядка использования сети Интернет и предъявляемых к обучающимся требований при работе в сети Интернет;

— доводит до классного руководителя информацию о нарушении обучающимся правил работы в сети Интернет;

— принимает необходимые меры по пресечению обращений к ресурсам, не имеющим отношения к образовательному процессу.

4. При обнаружении ресурса, который, по мнению учителя, содержит информацию, запрещенную для распространения в соответствии с законодательством Российской Федерации, или иного потенциально опасного для обучающихся контента, он сообщает об этом лицу, ответственному за работу Интернета и ограничение доступа.

5. В случае отказа доступа к ресурсу, разрешенному в ОУ, учитель также сообщает об этом лицу, ответственному за работу Интернета и ограничение доступа.

ИНСТРУКЦИЯ пользователя по компьютерной безопасности

1. Установить последние обновления операционной системы Windows.
2. Включить режим автоматической загрузки обновлений. (Пуск->Настройка->панель управления->Автоматическое обновление->Автоматически загружать и устанавливать на компьютер рекомендуемые обновления).
3. Активировать встроенный брандмауэр Windows (Пуск->Настройка->панель управления->Брандмауэр Windows->Включить).
4. Установить антивирусное программное обеспечение на каждый компьютер. Включить режим автоматического сканирования файловой системы. Включить режим ежедневной автоматической проверки всей файловой системы при включении компьютера. Активировать функцию ежедневного автоматического обновления антивирусных баз.
5. Ежедневно проверять состояние антивирусного программного обеспечения, а именно
 - Режим автоматической защиты должен быть включен постоянно.
 - Дата обновления антивирусных баз не должна отличаться более чем на несколько дней от текущей даты.
 - Просматривать журналы ежедневных антивирусных проверок. Контролировать удаление вирусов при их появлении.
6. Не реже одного раза в месяц посещать сайт <http://windowsupdate.microsoft.com> и проверять установлены ли последние обновления операционной системы.
7. Быть крайне осторожным при работе с электронной почтой. Категорически запрещается открывать присоединенные к письмам, полученным от незнакомых лиц, файлы.
8. Контролировать посещение Интернет сайтов пользователями. Не допускать посещения т.н. «хакерских», порно и других сайтов с потенциально вредоносным содержанием.
9. В обязательном порядке проверять антивирусным программным обеспечением любые внешние носители информации перед началом работы с ними.
10. При появлении признаков нестандартной работы компьютера («тормозит», на экране появляются и исчезают окна, сообщения, изображения, самостоятельно запускаются программы и т.п.) немедленно отключить компьютер от Ethernet сети, загрузить компьютер с внешнего загрузочного диска (CD, DVD) и произвести полную антивирусную проверку всех дисков компьютера. При появлении аналогичных признаков после проделанной процедуры переустановить операционную систему с форматированием системного раздела диска.

Приложение 9
к приказу директора школы
№ 119/1 от 29.08.2014

**Журнал контроля контентной фильтрации
в МОБУ «Кисельнинская средняя школа»**

Дата проверки	Ф.И.О. и должность проверяю- щего	Номер компьютера	Результаты проверки	Принятые меры	Подпись проверяю- щего

Приложение 10
к приказу директора школы
№ 119/1 от 29.08.2014

**Журнал проверок антивирусной защиты
в МОБУ «Кисельнинская средняя школа»**

Дата проверки	Ф.И.О. и должность проверяю- щего	Номер компьютера	Результаты проверки	Принятые меры	Подпись проверяю- щего

Правила использования сети Интернет в МОБУ «Кисельнинская средняя школа»

1. Общие положения

1.1. Настоящие Правила регулируют условия и порядок использования сети Интернет обучающимися, педагогическими работниками и иными работниками МОБУ «Кисельнинская средняя школа» (далее-ОУ).

1.2. Правила имеют статус локального нормативного акта ОУ. Если нормами действующего законодательства РФ предусмотрены иные требования, чем настоящими Правилами, применяются нормы действующего законодательства РФ.

1.3. Использование сети Интернет в ОУ подчинено следующим принципам:

- соответствие образовательным целям;
- способствование гармоничному формированию и развитию личности;
- уважение закона, авторских и смежных прав, а также иных прав, чести и достоинства других граждан и пользователей Интернет;
- приобретение новых навыков и знаний;
- расширение применяемого спектра учебных и наглядных пособий;
- социализация личности, введение в информационное общество.

2. Политика использования сети Интернет в ОУ

2.1. Использование сети Интернет в ОУ возможно исключительно при условии ознакомления и согласия лица, пользующегося сетью Интернет в ОУ, с настоящими Правилами.

2.2. Ознакомление и согласие удостоверяются подписью лица в листе ознакомления и согласия с Правилами. Ознакомление и согласие несовершеннолетнего удостоверяются, помимо его подписи, также подписью его родителя (законного представителя).

2.3. Директор школы (в отсутствие его - зам. директора школы по безопасности) является ответственным за обеспечение эффективного и безопасного доступа к сети Интернет, а также за внедрение соответствующих технических, правовых и др. механизмов в ОУ.

2.4. Непосредственное определение политики доступа в Интернет осуществляет Совет по вопросам регламентации доступа к информации в сети Интернет при МОБУ «Бережковская основная общеобразовательная школа»

2.5. Очередные собрания Совета проходят с периодичностью, установленной самим Советом.

Совет:

- принимает решение о разрешении / блокировании доступа к определенным ресурсам и (или) категориям ресурсов сети Интернет, содержащим информацию, не совместимую с задачами образовательного процесса, с учетом социокультурных особенностей региона;
- определяет характер и объем информации, публикуемой на интернет-ресурсах ОУ;
- дает директору школы рекомендации о назначении и освобождении от исполнения своих функций лиц, ответственных за непосредственный контроль безопасности работы в сети Интернет и соответствия ее целям и задачам образовательного процесса.

2.6. Во время занятий контроль за использованием обучающимися сети Интернет в соответствии с Правилами осуществляет учитель, ведущий занятие.

Учитель:

- наблюдает за использованием компьютера и сети Интернет обучающимися;
- запрещает дальнейшую работу обучающегося в сети Интернет в случае нарушения настоящих Правил и иных нормативных документов, регламентирующих использование сети Интернет в ОУ;

– принимает предусмотренные Правилами и иными нормативными документами меры для пресечения дальнейших попыток доступа к ресурсу / группе ресурсов, не совместимых с задачами образования.

2.7. Во время использования сети Интернет для свободной работы контроль осуществляет лицо, уполномоченное Советом ОУ.

Уполномоченное лицо:

– определяет время и место для свободной работы в сети Интернет обучающихся, педагогических и иных работников ОУ с учетом использования соответствующих технических мощностей ОУ в образовательном процессе, а также длительность сеанса работы одного человека;

– наблюдает за использованием компьютера и сети Интернет обучающимися;

– запрещает дальнейшую работу обучающегося в сети Интернет в случае нарушения настоящих Правил и иных нормативных документов, регламентирующих использование сети Интернет в ОУ;

– не допускает обучающегося к работе в сети Интернет в предусмотренных Правилами случаях;

– принимает предусмотренные Правилами и иными нормативными документами меры для пресечения дальнейших попыток доступа к ресурсу / группе ресурсов, не совместимых с задачами образования.

2.8. При использовании сети Интернет в ОУ осуществляется доступ только к ресурсам, содержание которых не противоречит законодательству РФ и не является несовместимым с целями и задачами образования и воспитания.

Проверка такого соответствия осуществляется с помощью специальных технических средств и программного обеспечения контекстного ограничения доступа, установленного в ОУ или предоставленного оператором услуг связи.

Использование сети Интернет в ОУ без применения данных технических средств и программного обеспечения (например, в случае технического отказа) допускается только с индивидуального разрешения директора школы.

Пользователи сети Интернет в ОУ понимают, что технические средства и программное обеспечение не могут осуществлять полную фильтрацию ресурсов сети Интернет в связи с частотой обновления ресурсов и осознают возможную опасность столкновения с ресурсом, содержание которого противоречит законодательству РФ и является несовместимым с целями и задачами образовательного процесса.

2.9. Решение о политике доступа к ресурсам / группам ресурсов сети Интернет принимает Совет ОУ самостоятельно либо с участием внешних экспертов, в качестве которых могут привлекаться:

– педагогические работники ОУ или других организаций (по согласованию);

– лица, имеющие специальные знания либо опыт работы в рассматриваемой области (по согласованию);

– представители Комитета по образованию администрации Волховского муниципального района;

– родители обучающихся, воспитанников.

При принятии решения эксперты руководствуются:

– законодательством РФ;

– специальными познаниями, в т. ч. полученными в результате профессиональной деятельности;

– опытом организации образовательного процесса с использованием информационных технологий и возможностей сети Интернет;

– интересами обучающихся, целями образовательного процесса;

– рекомендациями профильных органов и организаций в сфере классификации ресурсов сети Интернет.

2.10. Отнесение определенных категорий и / или ресурсов в соответствующие группы, доступ к которым регулируется техническими средствами и программным обеспечением контекстного

технического ограничения доступа к информации, технически осуществляется лицом, уполномоченным Советом ОУ.

2.11. Категории ресурсов, в соответствии с которыми определяется политика использования сети Интернет в ОУ, и доступ к которым регулируется техническими средствами и программным обеспечением контекстного технического ограничения доступа к информации, определяются в установленном порядке.

2.12. Принципами размещения информации на интернет-ресурсах ОУ являются:

- соблюдение действующего законодательства РФ, интересов и прав граждан;
- защита персональных данных обучающихся, педагогических работников и иных работников;
- достоверность и корректность информации.

2.13. Персональные данные об обучающихся (фамилия и имя, класс или группа, возраст, фотография, место жительства, телефоны и др. контакты, иные сведения личного характера) могут размещаться на интернет-ресурсах ОУ только с письменного согласия родителей (законных представителей). Персональные данные педагогических работников и иных работников ОУ размещаются на интернет-ресурсах ОУ только с письменного согласия работника, чьи персональные данные размещаются.

В информационных сообщениях о мероприятиях на сайте ОУ и его подразделений без согласия лица (законного представителя) могут быть упомянуты только его фамилия и имя.

При истребовании согласия представитель ОУ и / или совета ОУ разъясняет лицу возможные риски и последствия опубликования персональных данных. ОУ не несет ответственности в случае наступления таких последствий, если имелось письменное согласие лица (законного представителя) на опубликование персональных данных.

3. Процедура использования сети Интернет

3.1. Использование сети Интернет в ОУ осуществляется в целях образовательного процесса. В рамках развития личности, ее социализации и получения знаний в области сети Интернет и компьютерной грамотности лицо может осуществлять доступ к ресурсам необразовательной направленности.

3.2. По разрешению Ответственного лица обучающиеся (с согласия родителей, законных представителей), педагогические работники и другие сотрудники вправе:

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

3.3. Обучающемуся запрещается:

- находиться на ресурсах, содержание и тематика которых является недопустимой для несовершеннолетних и/или нарушающей законодательство РФ (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 загрузку файлов на компьютер ОУ без разрешения учителя;
- распространять оскорбительную, не соответствующую действительности, порочащую других лиц информацию, угрозы.

3.4. Ответственное лицо проверяет, отстранен ли обучающийся от самостоятельной работы в сети Интернет.

3.5. При случайном обнаружении лицом, работающим в сети Интернет, ресурса, содержимое которого не совместимо с целями образовательного процесса, он обязан незамедлительно сообщить о нем Ответственному лицу с указанием интернет-адреса (URL) и покинуть данный ресурс.

3.6. Ответственное лицо обязано:

- принять сообщение лица, работающего в сети Интернет;
- довести информацию до сведения Совета ОУ для оценки ресурса и принятия решения по политике доступа к нему;
- направить информацию о некатегоризированном ресурсе оператору технических средств и программного обеспечения технического ограничения доступа к информации (в течение суток);

– если обнаруженный ресурс явно нарушает законодательство РФ – сообщить о нем по специальной "горячей линии" для принятия мер в соответствии с законодательством РФ (в течение суток).

Передаваемая информация должна содержать:

- интернет-адрес (URL) ресурса;
- тематику ресурса, предположения о нарушении ресурсом законодательства РФ либо несовместимости с задачами образовательного процесса;
- дату и время обнаружения;
- информацию об установленных в ОУ технических средствах технического ограничения доступа к информации.