МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ « ДЕТСКИЙ САД №23 КОМБИНИРОВАННОГО ВИДА»

ПРИКАЗ

01.09.2014 г.Гатчина № 170/1

ОБ УТВЕРЖДЕНИИ ЛОКАЛЬНЫХ НОРМАТИВНЫХ АКТОВ ПО БЕЗОПАСНОЙ РАБОТЕ В СЕТИ ИНТЕРНЕТ

В целях соблюдения права обучающихся на защиту от информации, пропаганды и агитации, наносящих вред здоровью, нравственному и духовному развитию обучающихся, в соответствии с федеральным законом от 28.07.1998 года №124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации», на основании протокола № 1 от 29.08.2014 года заседания Педагогического совета

1. Утвердить РЕГЛАМЕНТ ОРГАНИЗАЦИИ ДОСТУПА К СЕТИ ИНТЕРНЕТ (приложение 1).
2. Утвердить РЕГЛАМЕНТ организации антивирусной защиты (приложение 2).
3. Утвердить РЕГЛАМЕНТ РАБОТЫ С ЭЛЕКТРОННОЙ ПОЧТОЙ (приложение 3).
4. Утвердить Классификатор информации, не соответствующий задачам образования (приложение 4).
5. Утвердить Классификатор информации, распространение которой среди детей определенных возрастных категорий ограничено (приложение 5).
6. Утвердить Классификатор информации, распространение которой запрещено в соответствии с законодательством РФ (приложение 6).
7. Утвердить ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ ПО КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ ПРИ РАБОТЕ В СЕТИ ИНТЕРНЕТ (приложение 7).
8. Контроль за исполнением данного приказа оставляю за собой.

Заведующий МБДОУ С.А.Исаева

С приказом ознакомлен(а):

приложение 1
к приказу № 170 \1 от 01.09.2014г.

РЕГЛАМЕНТ ОРГАНИЗАЦИИ ДОСТУПА К СЕТИ ИНТЕРНЕТ

Основные понятия:

Сеть Интернет представляет собой глобальное объединение компьютерных сетей и информационных ресурсов, принадлежащих множеству различных людей и организаций. Глобальная сеть Интернет предоставляет доступ к ресурсам различного содержания и направленности.
Пользователь сети Интернет – лицо, использующее ресурсы всемирной компьютерной сети.

При работе с ресурсами сети Интернет недопустимо:

Распространение защищаемых авторскими правами материалов, затрагивающих какой-либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и/или авторские и смежные с ним права третьей стороны.
Публикация, 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.

При работе с ресурсами Интернет запрещается:

Загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным пакетом.
Использовать программные и аппаратные средства, позволяющие получить доступ к ресурсам сети Интернет, содержание которых не имеет отношения к образовательному процессу, содержащим информацию, несовместимую с задачами образования и воспитания учащихся,а также к ресурсам, содержание и направленность которых запрещены международным и Российским законодательством, включая материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и т.д.

ОБЩИЕ ПОЛОЖЕНИЯ

Использование сети Интернет в образовательном учреждении направлено на решение задач учебно-воспитательного процесса.
Доступ к сети Интернет должен осуществляться только с использованием лицензионного программного обеспечения или программного обеспечения, разрешенного для свободного использования.
Настоящий Регламент регулирует условия и порядок использования сети Интернет в

образовательном учреждении (ОУ).
Настоящий Регламент имеет статус локального нормативного акта образовательного учреждения.

Организация использования сети Интернет в образовательном учреждении

Вопросы использования возможностей сети Интернет в учебно-воспитательном процессе рассматриваются на педагогическом совете. Педагогический совет утверждает Правила использования сети Интернет на учебный год. Правила вводятся в действие приказом руководителя ОУ.
Правила использования сети Интернет разрабатываются педагогическим советом ОУ на основе данного регламента самостоятельно либо с привлечением внешних экспертов, в качестве которых могут выступать преподаватели других общеобразовательных учреждений, имеющие опыт использования Интернета в образовательном процессе, специалисты в области информационных технологий, представители муниципальных органов управления образованием, родители обучающихся.
При разработке правил использования сети Интернет педагогический совет руководствуется:

- законодательством Российской Федерации, региональными и муниципальными нормативно-правовыми актами;
- целями образовательного процесса;
- рекомендациями профильных органов и организаций в сфере классификации ресурсов Сети;
- интересами обучающихся.

Руководитель образовательного учреждения отвечает за обеспечение пользователям (сотрудникам и обучающимся) эффективного и безопасного доступа к сети Интернет. Для обеспечения доступа к Сети участникам образовательного процесса руководитель ОУ назначает своим приказом ответственного из числа сотрудников образовательного учреждения за организацию работы с Интернетом и ограничение доступа.
Педагогический совет ОУ:

- принимает решение о разрешении/блокировании доступа к определенным ресурсам и (или) категориям ресурсов сети Интернет;
- определяет объем и характер информации, публикуемой на Интернет-ресурсах ОУ.

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.

Во время свободного доступа обучающихся к сети Интернет вне учебных занятий, контроль использования ресурсов Интернета осуществляют работники ОУ, определенные приказом его руководителя. Работник образовательного учреждения:

- наблюдает за использованием компьютера в сети Интернет обучающимися;
- принимает меры по пресечению обращений к ресурсам, не имеющим отношения к образовательному процессу.

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 ОУ или

предоставленного оператором услуг связи.
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 ОУ.
При обнаружении указанной информации пользователю необходимо сообщить об этом ответственному за использование сети Интенет в ОУ, указав при этом адрес ресурса.
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 в ОУ правилами, обеспечивается назначенным работником ОУ.
Принципы размещения информации на Интернет-ресурсах ОУ призваны обеспечить:

- соблюдение действующего законодательства Российской Федерации, интересов и прав граждан;
- защиту персональных данных обучающихся, преподавателей и сотрудников ОУ;
- достоверность и корректность информации.

Персональные данные обучающихся (включая фамилию и имя, класс/группу/год обучения, возраст, фотографию, данные о месте жительства, телефонах и пр., иные сведения личного характера) могут размещаться на интернет-ресурсах только с письменного согласия лица, чьи персональные данные размещаются.
В информационных сообщениях о мероприятиях, размещенных на сайте ОУ 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.
При получении согласия на размещение персональных данных, представитель ОУ обязан разъяснить возможные риски и последствия их опубликования. ОУ не несет ответственности за такие последствия, если предварительно было получено письменное согласие лица (его законного представителя) на опубликование персональных данных.

Права, обязанности и ответственность пользователей

Преподаватели, сотрудники и обучающихся могут бесплатно пользоваться доступом к глобальным Интернет-ресурсам по разрешению лица, назначенного ответственным за организацию в ОУ работы сети Интернет и ограничению доступа.
Пользователям запрещается:

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

Пользователи несут ответственность:
1. За содержание передаваемой, принимаемой и печатаемой информации.
2. За нанесение любого ущерба оборудованию в «точке доступа к Интернету» (порча имущества, вывод оборудования из рабочего состояния) пользователь несет материальную ответственность.
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.

Пользователи имеют право:
1. Работать в сети Интернет в течение периода времени, определенного Правилами ОУ.
2. Сохранять полученную информацию на съемном накопителе.
3. Размещать собственную информацию в сети Интернет на Интернет-ресурсах ОУ.

приложение 2
к приказу №170 \1от 01.09.2014г.

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 Учреждения к непродуктивным Интернет-ресурсам и контроля их электронной переписки.

Основополагающими требованиями к системе антивирусной защиты Учреждения 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.
- Мероприятия, направленные на решение задач по антивирусной защите:

установка только лицензированного программного обеспечения либо бесплатное антивирусное программное обеспечение, идущее в комплекте с подлинной операционной системой (типа Microsoft Security Essentials (сеть до 10 рабочих станций) или Microsoft Forefront Endpoint Protection (сеть более 10 рабочих станций)), поддерживающее работу с пользовательскими профилями.

- 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 Учреждения 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.

Технологические инструкции

1.1. В учреждении руководителем 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 руководителя Учреждения.

1.2. В Учреждении может использоваться только лицензионное антивирусное программное обеспечение либо свободно-распространяемое программное обеспечение.

1.3. 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).

1.4. 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) Учреждения.

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 руководителя Учреждения или лицо, им назначенное.

3.2. Ответственность за проведение мероприятий антивирусного контроля в Учреждении возлагается на ответственного за обеспечение антивирусной защиты, соблюдение требований настоящей Инструкции при работе на персональных компьютерах возлагается на ответственных за кабинет, где используется данный компьютер.

приложение 3
к приказу №170 \1 от 01.09.2014г.

РЕГЛАМЕНТ РАБОТЫ С ЭЛЕКТРОННОЙ ПОЧТОЙ

ОБЩИЕ ПОЛОЖЕНИЯ

1. Электронный почтовый ящик(и) учреждения может использоваться только в служебных целях.

Запрещается: рассылка личных почтовых сообщений, спама, вложений с вирусами, сообщений неэтичного или противозаконного характера, сведений для служебного пользования и другой конфиденциальной информации (без официально запроса) и т.п.

2. По электронной почте образовательного учреждения производится обмен информацией законодательного, нормативно-правового, учебного, учебно-методического характера между учреждениями образования, органами управления образованием разных уровней, поставщиками оборудования и материалов, подрядчиками, поставщиками услуг и другими организациями, предприятиями и учреждениями, связанными с образовательным учреждением договорными или иными обязательствами.
3. Для обработки, передачи и приема информации по электронной почте в учреждениях образования приказом директора назначается ответственное лицо.
4. Пользователи электронной почты образовательного учреждения должны строго соблюдать локальные правила и инструкции по работе с электронной корреспонденцией, а также данный Регламент.

приложение 4

к приказу № 170 \1от 01.09.2014г.

Классификатор информации, не соответствующий задачам образования

№ п/п	Тематическая категория	Содержание
1	Алкоголь.	Реклама алкоголя, пропоганда потребления алкоголя. Сайты компаний, производящих алкогольную продукцию.
2	Баннеры и рекламные программы.	Баннерные сети, всплывающая реклама, рекламные программы.
3	Вождение и автомобили (ресурсы данной категории, не имеющие отношения к образовательному процессу).	Не имеющая отношения к образовательному процессу информация об автомобилях и других транспортных средствах, вождении, автозапчастях, автомобильных журналах, техническом обслуживании, аксессуарах к автомобилям.
4	Досуг и развлечения (ресурсы данной категории, не имеющие отношения к образовательному процессу).	Не имеющая к образовательному процессу информация: - фотоальбомы и фотоконкурсы; - рейтинги открыток, гороскопов, сонников; - гадания, магия, астрология; - тв – программы; - прогнозы погоды; - тесты, конкурсы онлайн; - туризм, путешествия; - тосты, поздравления; - кроссворды, сканворды, ответы к ним; - фантастика; - кулинария, рецепты, диеты; - мода, одежда, обувь, модные аксессуары, показы мод; - тексты песен, кино, киноактеры, расписания концертов, спектаклей, кинофильмов, заказ билетов в театры, кино и т.п.; - о дачах, участках, огородах, садах, цветоводстве, животных, питомцах, уходе за ними; - о рукоделии, студенческой жизни, музыке и музыкальных направлениях, группах,

		увлечениях, хобби, коллекционировании; - о службах знакомств, размещении объявлений онлайн; - анекдоты, «приколы», слухи; - о сайтах и журналах для женщин и для мужчин; - желтая пресса, онлайн – ТВ, онлайн – радио; - о знаменитостях; - о косметике, парфюмерии, прическах, ювелирных украшениях.
5	Здоровье и медицина (ресурсы данной категории, не имеющие отношения к образовательному процессу).	Не имеющая отношения к образовательному процессу информация о шейпинге, фигуре, похудении, медицине, медицинских учреждениях, лекарствах, оборудовании, а также иные материалы на тему «Здоровье и медицина», которые, являясь академическими, по сути могут быть также отнесены к другим категориям (порнография, трупы и т.п.).
6	Компьютерные игры (ресурсы данной категории, не имеющие отношения к образовательному процессу).	Не имеющая отношения к образовательному процессу информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети «Интернет») по тематике компьютерных игр, не соответствующая задачам образования, такая как порталы браузерных игр, массовые многопользовательские ролевые онлайн игры (MMORPG), массовые многопользовательские игры, основанные на имитации боевых или противоправных действий, советы для игроков и ключи для установки и прохождения игр, игровые форумы и чаты.
7	Корпоративные сайты, интернет-представительства негосударственных учреждений (ресурсы данной категории, не имеющие отношения к образовательному процессу).	Содержащие информацию, не имеющую отношения к образовательному процессу, сайты коммерческих фирм, компаний, предприятий, организаций.

8	Ресурсы, базирующиеся либо ориентированные на обеспечение анонимности распространителей и потребителей информации.	Анонимные форумы, чаты, доски объявлений и гостевые книги, такие как имиджборды, анонимайзеры, программы, обеспечивающие анонимизацию сетевого трафика в сети «Интернет» (tor, I2P).
9	Банки рефератов, дипломных работ, эссе, за исключением соответствующих задачам образования.	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети «Интернет»), представляющая собой банки готовых рефератов, дипломных работ, эссе, за исключением печатных и электронных образовательных и информационных ресурсов, создаваемых в организациях, осуществляющих образовательную деятельность.
10	Личная и немодерируемая информация.	Немодерируемые форумы, доски объявлений и конференции, гостевые книги, базы данных, содержащие личную информацию (адреса, телефоны и т.п.), личные странички, дневники, блоги.
11	Онлайн – казино и тотализаторы.	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети «Интернет»), содержащая информацию об электронных казино, тотализаторах, играх на деньги.
12	Отправка SMS с использованием интернет-ресурсов.	Сайты, предлагающие услуги по отправке SMS – сообщений.
13	Мошеннические сайты.	Сайты, навязывающие платные услуги на базе SMS – платежей, сайты, обманным путем собирающие личную информацию (фишинг).
14	Модерируемые доски объявлений (ресурсы данной категории, не имеющие отношения к образовательному процессу).	Сайты, содержащие информацию, не имеющую отношения к образовательному процессу, модерируемые доски сообщений/объявлений, а также модерируемые чаты.
15	Магия, колдовство, чародейство, ясновидение, приворот по фото, теургия,	Информационая продукция, оказывающая психологичское воздействие на детей, при которой ребенок обращается к тайным силам

	волшебство, некромантия, тоталитарные секты.	с целью влияния на события, а также реального или кажущегося воздействия на состояние.
16	Неприличный и грубый юмор.	Неэтичные анекдоты и шутки, в частности обыгрывающие особенности физиологии человека.
17	Нижнее белье, купальники.	Сайты, на которых рекламируется нижнее белье, купальники, а также присутствуют образы полуобнаженных людей.
18	Обеспечение анонимности пользователя, обход контентных фильтров.	Сайты, предоставляющие инструкции по обходу прокси и доступа к запрещенным страницам; Peer–to–Peer программы, сервисы бесплатных прокси-серверов, сервисы, дающие пользователю анонимность.
19	Платные сайты.	Сайты, на которых вывешено объявление о платности посещения веб-страниц.
20	Поиск работы, резюме, вакансии (ресурсы данной категории, не имеющие отношения к образовательному процессу).	Содержащие информацию, не имеющую отношения к образовательному процессу, интернет-представительства кадровых агенств, банки вакансий и резюме.
21	Поисковые системы (ресурсы данной категории, не имеющие отношения к образовательному процессу).	Содержащие информацию, не имеющую отношения к образовательному процессу, интернет-каталоги, системы поиска и навигации в сети «Интернет».
22	Религия и атеизм (ресурсы данной категории, не имеющие отношения к образовательному процессу).	Сайты, содержащие информацию, не имеющую отношения к образовательному процессу, информацию религиозной и антирелигиозной направленности.
23	Системы поиска изображений.	Системы для поиска изображений, не имеющих отношения к образовательному процессу, в сети «Интернет» по ключевому слову или словосочетанию.
24	СМИ (ресурсы данной категории, не имеющие отношения к образовательнму процессу).	СМИ, содержащие новостные ресурсы и сайты СМИ (радио, телевидения, печати), не имеющие отношения к образовательному процессу.
25	Реклама табака, пропаганда потребления табака.	Сайты, пропагандирующие потребление табака; реклама табака и изделий из него.

26	Чаты (ресурсы данной категории, не имеющие отношения к образовательному процессу).	Не имеющие отношения к образовательному процессу сайты для анонимного общенияи в режиме онлайн.
27	Убийства, насилие.	Сайты, содержащие описание или изображение убийств, мертвых тел, насилия и т.п.
28	Торговля и реклама (ресурсы данной категории, не имеющие отношения к образовательному процессу).	Не имеющие отношения к образовательному процессу сайты следубщих категорий: аукционы, онлайн-распродажи, интернет-магазины, каталоги товаров и цен, электронная коммерция, модели мобильных телефонов, юридические услуги, полиграфия, типографии и их услуги, таможенные услуги, охранные услуги, иммиграционные услуги, услуги по переводу текста на иностранные языки, канцелярские товары, налоги, аудит, консалтинг, деловая литература, дом, ремонт, строительство, аренда/покупка/продажа недвижимости, продажа услуг мобильной связи (например, картинки и мелодии для сотовых телефонов), заработок в сети «Интернет», электронная коммерция.

*рекомендуется исключить из обработки систем контент – фильтрации образовательные ресурсы, относящиеся к домену edu.ru

приложение 5
к приказу №170 \1 от 01.09.2014г.

Классификатор информации, распространение которой среди детей определенных возрастных категорий ограничено

№ п/п	Тематическая категория	Содержание
1	Информация, представляемая в виде изображения жестокости.	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети «Интернет»), содержащая описание, фотографии, рисунки, видеоматериалы сцен жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия.
2	Информация, вызывающая у детей страх, ужас или панику.	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети «Интернет»), содержащая описание, фотографии, рисунки, видеоматериалы, в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий.
3	Информация сексуального характера.	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети «Интернет»), представляемая в виде изображений, видеоматериалов, описания половых отношений между мужчиной и женщиной.
4	Информация, содержащая нецензурную лексику.	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети «Интернет»), содержащая бранные слова и выражения, не относящиеся к нецензурной лексике.

Приложение 6
к приказу № 170 \1 от 01.09.2014г.

Классификатор информации, распространение которой запрещено в соответствии с законодательством РФ		
№ п/п	Тематическая категория	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 террорестической деятельности, оправдывающая терроризм, содержащая другие экстремистские материалы.
3	Злоупотребление свободой СМИ – наркотические средства.	Сведения о способах, методах разработки, изготовления, местах приобретения наркотических средств, психотропных веществ и их прекурсоров, пропоганда каких-либо преимуществ использования отдельных наркотических средств, психотропных веществ, их аналогов и прекурсов.
4	Злоупотребление свободой СМИ – информация с ограниченным доступом.	Сведения о специальных средствах, технических приемах и тактике проведения контртеррористических операций.
5	Злоупотребление СМИ – скрытое воздействие.	Информация, содержащая скрытые вставки и иные технические способы воздействия на подсознание людей и (или) оказывающая вредное влияние на их здоровье.
6	Экстремистские материалы или экстремистская	А) Экстремистские материалы, то есть предназначенные для обнародования документов или информация, призывающие к

	деятельность (экстремизм).	осуществлению экстремистской деятельности, либо обосновывающие или оправдывающие необходимость осуществления такой деятельности, в том числе труды руководителей национал-социалистической рабочей партии Германии, фашисткой 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 деятельность по распространению материалов (произведений), содержащих хотя бы один из следующих признаков: - насильственное изменение основ конституционного строя и нарушение целостности 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, расовой, национальной или религиозной ненависти либо вражды, а равно по мотивам ненависти либо вражды в отношении какой-либо социальной группы; - пропаганда исключительности, превосходства либо неполноценности

		граждан по признаку их отношения к религии, социальной, расовой, национальной, религиозной или языковой пренадлежности; - воспрепятствование законной деятельности органов государственной власти, избирательных комиссий, а также законной деятельности должностных лиц указанных органов, комиссий, сопровождаемое насилием или угрозой его применения; - публичная клевета 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, сопровождаемая 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 угроза применения насилия в отношении представлителя 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 неприличной форме); - публичные призывы к осуществлению террорестической 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 социального, расового, национального и религиозного неравенства; - публичные призывы к развязыванию агрессивной войны.
9	Ненадлежащая реклама.	Информация, содержащая рекламу алкогольной продукции и табачных изделий.
10	Информация с ограниченным доступом.	Информация, составляющая государственную, коммерческую, служебную или иную охраняемую законом тайну.

приложение 7
к приказу №170 \1 от 01.09.2014г.

ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ ПО КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ ПРИ РАБОТЕ В СЕТИ ИНТЕРНЕТ

ОБУЧАЮЩИМСЯ:

1. Обязанности обучающегося – пользователя сети Интернет.
   1.1 Обучающийся обязан выполнять требования лица, уполномоченного контролировать использование сити Интернет.
   1.2 Соблюдать тишину, чистоту и порядок в компьютерном классе и выполнять указания ица, уполномоченного контролировать использование сити Интернет.
   1.3 Посещать Интернет-ресурсы только образовательной направленности.
   1. 4 Сообщить ответственному лицу о случайном попадании на ресурс, явно не соответствующий образовательной направленности и/или нарушающий законодательствол РФ, с указанием Интернет-адреса ресурса (URL), затем немедленно покинуть ресурс.

2.Обучающемуся – пользователю сети Интернет запрещается:
   - Посещать сайты, содержащие информацию необразовательной направленности (порнографическую, антигосударственную, со сценами насилия и т.п.), участвовать в нетематических форумах, чатах, конференциях, социальных сетях.
   - Устанавливать дополнительное программное обеспечение, как полученное в Интернете, так и любое другое, без согласования с ответственным лицом.
   - Изменять конфигурацию компьютера, в том числе менять системные настройки и настройки программ, установленных на нем, а также включать, выключать и перезагружать компьютер без согласования с ответственным лицом.
   - Осуществлять действия, направленные на “взлом” любых компьютеров.

3. Права обучающегося – пользователя сети Интернет
   3.1.Обучающийся имеет право во время занятия работать в сети Интернет в течение времени, отведенного ответственным лицом.
   3.2.Получить учетную запись электронной почты на интернет-ресурсе.
   3.3.Сохранять полученную информацию на внешнем носителе.

4. Ответственность обучающегося - пользователя сети Интернет
   4.1. Пользователь несет ответственность за содержание передаваемой, принимаемой и распечатываемой информации.
   4.2. Лица, не соблюдающие настоящую инструкцию, лишаются права работы в сети Интернет.
   4.3. При нанесении любого ущерба «точке доступа к Интернету» (порча имущества, вывод оборудования из рабочего состояния) пользователь несет материальную ответственность.

СОТРУДНИКАМ:

1. Обязанности сотрудника – пользователя сети Интернет.
   1.1. Использовать ресурсы сети Интернет в образовательных целях.
   1.2. Уважать законы, авторские права, честь и достоинство других пользователей

сети Интернет.

1.3. Использовать ресурсы сети Интернет для приобретения новых знаний и навыков в области образования, расширения спектра учебных и наглядных пособий, содействия гармоничному формированию и развитию личности обучающегося, ее социализации, введению в информационное общество.

1.4. Осуществлять контроль за использованием обучающимися ресурсов сети Интернет во время занятий: наблюдать за использованием компьютера и сети Интернет, запрещать работу обучающегося в случае нарушения им настоящей инструкции и других документов, регламентирующих использование сети Интернет, принимать меры по пресечению попыток доступа к ресурсам, несовместимым с задачами образования.

ИНТЕРНЕТ-РЕСУРСЫ НЕОБРАЗОВАТЕЛЬНОЙ НАПРАВЛЕННОСТИ

1. Участники процесса использования сети Интернет в ОУ осознают, что ОУ не несет ответственности за случайный доступ к информации, содержание которой противоречит законодательству РФ и является несовместимым с целями и задачами образовательного процесса, размещенной не на Интернет-ресурсах ОУ.
2. Пользователю 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, распространять рекламную, коммерческую или схожую по направленности информацию, участвовать в чатах, конференциях, форумах необразовательной направленности, распространять оскорбительную, не соответствующую действительности, порочащую других лиц информацию, угрозы.
3. При случайном обнаружении лицом, работающим в сети Интернет, ресурса, содержимое которого несовместимо с целями образовательного процесса, он обязан незамедлительно сообщить о таком ресурсе Уполномоченному лицу с указанием Интернет-адреса (URL) и покинуть данный ресурс.

ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ ПО КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ ПРИ РАБОТЕ В СЕТИ ИНТЕРНЕТ

ОБУЧАЮЩИМСЯ:

1. Обязанности обучающегося – пользователя сети Интернет.

1.1 Обучающийся обязан выполнять требования лица, уполномоченного контролировать использование сити Интернет.

1.2 Соблюдать тишину, чистоту и порядок в компьютерном классе и выполнять указания ица, уполномоченного контролировать использование сити Интернет.

1.3 Посещать Интернет-ресурсы только образовательной направленности.

1. 4 Сообщить ответственному лицу о случайном попадании на ресурс, явно не соответствующий образовательной направленности и/или нарушающий законодательствол РФ, с указанием Интернет-адреса ресурса (URL), затем немедленно покинуть ресурс.

3.Обучающемуся – пользователю сети Интернет запрещается:

- Посещать сайты, содержащие информацию необразовательной направленности (порнографическую, антигосударственную, со сценами насилия и т.п.), участвовать в нетематических форумах, чатах, конференциях, социальных сетях.

- Устанавливать дополнительное программное обеспечение, как полученное в Интернете, так и любое другое, без согласования с ответственным лицом.
- Изменять конфигурацию компьютера, в том числе менять системные настройки и настройки программ, установленных на нем, а также включать, выключать и перезагружать компьютер без согласования с ответственным лицом.
- Осуществлять действия, направленные на “взлом” любых компьютеров.

5. Права обучающегося – пользователя сети Интернет
   3.4.Обучающийся имеет право во время занятия работать в сети Интернет в течение времени, отведенного ответственным лицом.
   3.5.Получить учетную запись электронной почты на интернет-ресурсе.
   3.6.Сохранять полученную информацию на внешнем носителе.

6. Ответственность обучающегося - пользователя сети Интернет
   4.1. Пользователь несет ответственность за содержание передаваемой, принимаемой и распечатываемой информации.
   4.2. Лица, не соблюдающие настоящую инструкцию, лишаются права работы в сети Интернет.
   4.3. При нанесении любого ущерба «точке доступа к Интернету» (порча имущества, вывод оборудования из рабочего состояния) пользователь несет материальную ответственность.

СОТРУДНИКАМ:

2. Обязанности сотрудника – пользователя сети Интернет.
   1.5. Использовать ресурсы сети Интернет в образовательных целях.
   1.6. Уважать законы, авторские права, честь и достоинство других пользователей сети Интернет.
   1.7. Использовать ресурсы сети Интернет для приобретения новых знаний и навыков в области образования, расширения спектра учебных и наглядных пособий, содействия гармоничному формированию и развитию личности обучающегося, ее социализации, введению в информационное общество.
   1.8. Осуществлять контроль за использованием обучающимися ресурсов сети Интернет во время занятий: наблюдать за использованием компьютера и сети Интернет, запрещать работу обучающегося в случае нарушения им настоящей инструкции и других документов, регламентирующих использование сети Интернет, принимать меры по пресечению попыток доступа к ресурсам, несовместимым с задачами образования.

ИНТЕРНЕТ-РЕСУРСЫ НЕОБРАЗОВАТЕЛЬНОЙ НАПРАВЛЕННОСТИ

1. Участники процесса использования сети Интернет в ОУ осознают, что ОУ не несет ответственности за случайный доступ к информации, содержание которой противоречит законодательству РФ и является несовместимым с целями и задачами образовательного процесса, размещенной не на Интернет-ресурсах ОУ.
2. Пользователю 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, распространять рекламную, коммерческую или схожую по направленности информацию, участвовать в чатах, конференциях, форумах

необразовательной направленности, распространять оскорбительную, не соответствующую действительности, порочащую других лиц информацию, угрозы.

3. При случайном обнаружении лицом, работающим в сети Интернет, ресурса, содержимое которого несовместимо с целями образовательного процесса, он обязан незамедлительно сообщить о таком ресурсе Уполномоченному лицу с указанием Интернет-адреса (URL) и покинуть данный ресурс.