Информационная безопасность

МАОУ СШ №8

Медиаграмотность

- развитие критического анализа содержания информации и привития коммуникативных навыков,
- содействие профессиональной подготовке обучающихся и их педагогов в целях позитивного и ответственного использования ими информационных и коммуникационных технологий и услуг.
- грамотное использование обучающимися и их преподавателями инструментов, обеспечивающих доступ к информации,

Нормативная база

Федеральный закон № 436-ФЗ

«О защите детей от информации, причиняющей вред их здоровью и развитию»

Устанавливает правила медиабезопасности детей при обороте на территории России продукции средств массовой информации, печатной, аудиовизуальной продукции на любых видах носителей, программ для ЭВМ и баз данных, а также информации, размещаемой в информационно-телекоммуникационных сетях и сетях подвижной радиотелефонной связи.

Нормативная база

- **Создание и распространение вредоносных программ (в том числе вирусов) преследуется в России согласно Уголовному кодексу РФ (глава 28, статья 273)**

- **Существует Доктрина информационной безопасности РФ, согласно которой в России должен проводиться правовой ликбез в школах и вузах при обучении информатике и компьютерной грамотности по вопросам защиты информации в ЭВМ, борьбы с компьютерными вирусами, детскими порносайтами и обеспечению информационной безопасности в сетях ЭВМ.**

Информационная безопасность обучающихся

это состояние защищенности обучающихся, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию

(Федеральный закон от 29.12.2010 №436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" (в ред. Федерального закона от 28.07.2012 N 139-ФЗ)).

Виды он-лайн угроз

- **Виртуальные знакомые и друзья**
- **Кибербуллинг *(cyberbullying) – подростковый виртуальный террор***
- **Откровенные материалы сексуального характера**
- **Буллицид – *доведение ребенка до самоубийства путем психологического насилия***
- **Электронные ресурсы, содержащие материалы экстремистского и террористического характера.**
- **Электронные ресурсы, созданные и поддерживаемые деструктивными религиозными сектами.**
- **Компьютерные мошенники, спамеры, фишеры.**

Виды он-лайн угроз

- ***Пропаганда наркотиков, насилия и жестокости, суицидального поведения, абортов, самоповреждений***
- ***Сомнительные развлечения:онлайн-игры, пропагандирующие секс, жестокость и насилие.***
- ***Болезненное пристрастие к участию в сетевых процессах, так называемой "Интернет-зависимости"***
- ***Социальные сети и блоги, на которых ребенок оставляет о себе немало настоящей информации, завязывает небезопасные знакомства, нередко подвергается незаметной для него деструктивной психологической и нравственно-духовной обработке.***

PEGI логотипы

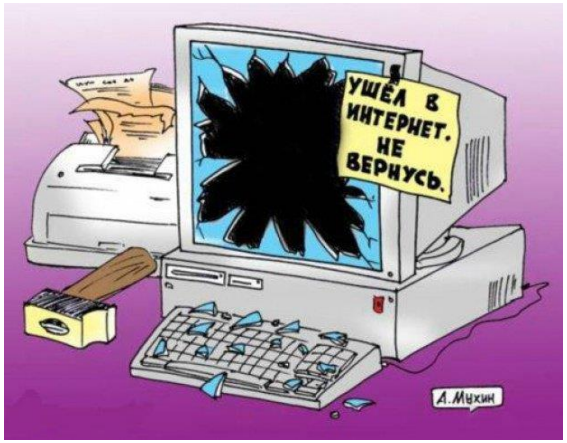
	**Bad Language - Ненормативная лексика** **Игра содержит грубые и непристойные выражения.**
	**Discrimination - Дискриминация** **Присутствие в продукте сцен или материалов, которые могут порочить или дискриминировать некоторые социальные группы.**
	**Fear - Страх:** **Материалы игры могут оказаться страшными и пугающими для маленьких детей.**
	**Gambling - Азартные игры** **В игре есть возможность сыграть в азартные игры и сделать ставку, в том числе — реальными деньгами.**
	**Sexual Content – Непристойности** **В игре присутствует обнажение и/или встречаются сцены с сексуальными отношениями.**
	**Violence - Насилие** **Игра изобилует сценами с применением насилия.**

Интернет-зависимость

- **Навязчивый веб-серфинг — бесконечные путешествия по Всемирной паутине, поиск информации.**
- **Пристрастие к виртуальному общению и виртуальным знакомствам — большие объёмы переписки, постоянное участие в чатах, веб-форумах, избыточность знакомых и друзей в Сети.**
- **Игровая зависимость — навязчивое увлечение компьютерными играми по сети.**
- **Навязчивая финансовая потребность — игра по сети в азартные игры, ненужные покупки в интернет-магазинах или постоянные участия в интернет-аукционах.**
- **Пристрастие к просмотру фильмов через интернет, когда больной может провести перед экраном весь день не отрываясь из-за того, что в сети можно посмотреть практически любой фильм или передачу.**

Признаки Интернет-зависимости:

- чрезмерное, немотивированное злоупотребление длительностью работы в сети, не обусловленное профессиональной, учебной или иной созидательной деятельностью;
- использование Интернета как преобладающего средства коммуникации;
- создание и эксплуатация виртуальных образов, крайне далеких от реальных;
- влечение к Интернет-играм и(или) созданию вредоносных программ (без какой-либо цели);
- субъективно воспринимаемая невозможность обходиться без работы в сети

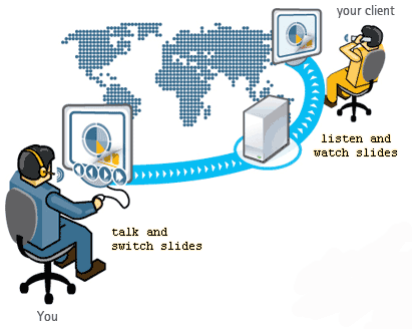


Это важно знать!

- **Когда ты регистрируешься на сайтах, не указывай личную информацию (номер мобильного телефона, адрес места жительства и другие данные).**
- **Используй веб-камеру только при общении с друзьями. Проследи, чтобы посторонние люди не имели возможности видеть ваш разговор. Научись самостоятельно включать и выключать веб-камеру.**
- **Ты должен знать, что если ты публикуешь фото или видео в интернете — каждый может посмотреть их.**

Это важно знать!

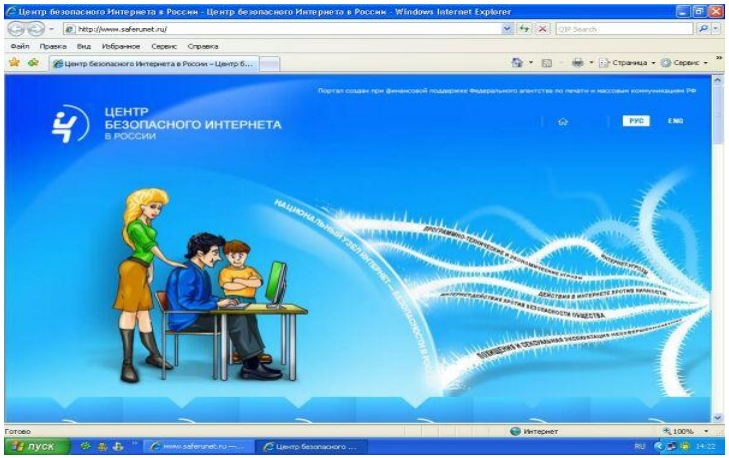
- **Не публикуй фотографии, на которых изображены другие люди. Делай это только с их согласия.**
- **Публикуй только такую информацию, о публикации которой не пожалеешь.**
- **Нежелательные письма от незнакомых людей называются «Спам». Если ты получил такое письмо, не отвечай на него. Если ты ответишь на подобное письмо, отправитель будет знать, что ты пользуешься своим электронным почтовым ящиком, и будет продолжать посылать тебе спам.**



Это важно знать!

- **Если тебе пришло сообщение с незнакомого адреса, его лучше не открывать. Подобные письма могут содержать вирусы.**
- **Не добавляй незнакомых людей в свой контакт-лист в ICQ.**
- **Если тебе приходят письма с неприятным или оскорбляющим тебя содержанием, если кто-то ведет себя в твоем отношении неподобающим образом, сообщи об этом взрослым.**
- **Если человек, с которым ты познакомился в интернете, предлагает тебе встретиться в реальной жизни, то предупреди его, что придешь навстречу со взрослым. Если твой виртуальный друг действительно тот, за кого он себя выдает, он нормально отнесется к твоей заботе о собственной безопасности.**

Это важно знать!



- **Если у тебя возникли вопросы или проблемы при работе в онлайн-среде,**
- **обязательно расскажи об этом кому-нибудь, кому ты доверяешь. Твои родители или другие взрослые могут помочь или дать хороший совет о том, что тебе делать. Любую проблему можно решить! Ты можешь обратиться на линию помощи «Дети онлайн» по телефону: 88002500015 (по России звонок бесплатный) или по**
- **e-mail: helpline@detionline.org.**
- **Специалисты посоветуют тебе, как поступить.**

Интернет-этикет

- **Узнайте** правила прежде, чем что-нибудь сказать или сделать.
- **Думайте** прежде, чем что-либо напечатать. Удостоверьтесь, что Вы говорите приемлемые вещи, которые не приведут к разгоревшемуся конфликту. Единственное, в чем Вы можете не сомневаться – это в том, что все, сказанное Вами в Интернете, может вернуться и неотступно преследовать Вас.
- **Не относитесь** критически к другим, особенно к новичкам, даже если они нарушают правила. Если Вы должны помочь кому-то или исправить кого-то, сделайте это по электронной почте, а не на общественном форуме (например, в чате). Помните, что и Вы когда-то были новичком.
- **Не тратьте** время других пользователей впустую. Не посылайте цепочку электронных писем, не передавайте киберслухи, не разыгрывайте других, не рассылайте спам.
- **Защищайте** личную жизнь и личную информацию других пользователей. Не публикуйте в онлайне чей-либо адрес электронной почты без разрешения владельца. Вместо этого можно использоваться опцию «Отправить по электронной почте». Не используйте без разрешения чужой пароль.
- **Не присваивайте** вещи, не платя за них (в основном это касается условно-бесплатного программного обеспечения).


Будь начеку!

- **Если ты видишь или знаешь, что твоего друга запугивают в онлайне, поддержи его и сообщи об этом взрослым. Ведь ты бы захотел, чтобы он сделал то же самое для тебя.**
- **Не посылай сообщения или изображения, которые могут повредить или огорчить кого-нибудь. Даже если не ты это начал, тебя будут считать участником круга запугивания.**
- **Всегда будь начеку, если кто-то, особенно незнакомец, хочет поговорить с тобой о взрослых отношениях. Помни, что в сети никогда нельзя быть уверенным в истинной сущности человека и его намерениях. Обращение к ребенку или подростку с сексуальными намерениями всегда является серьезным поводом для беспокойства. Ты должен рассказать об этом взрослому, которому доверяешь, для того чтобы вы могли сообщить о неприятной ситуации в правоохранительные органы.**
- **Если тебя заманили или привлекали обманом к совершению действий сексуального характера или к передаче сексуальных изображений с тобой, ты обязательно должен рассказать об этом взрослому, которому доверяешь, для того чтобы получить совет или помощь. Ни один взрослый не имеет права требовать подобного от ребенка или подростка – ответственность всегда лежит на взрослом.**

Установи свои рамки

- **Используя социальные сети, либо любые другие онлайн-сервисы, позаботься о своей конфиденциальности и конфиденциальности твоей семьи и друзей.**
- **Если ты зарегистрировался на сайте социальной сети, используй настройки конфиденциальности, для того чтобы защитить твой онлайн-профиль таким образом, чтобы только твои друзья могли его просматривать. Попроси своих родителей помочь с настройками, если сам затрудняешься. Это правило очень важно.**

Установи свои рамки

- **Храни свои персональные данные в тайне, особенно при общении во взрослых социальных сетях. Используй ник вместо своего настоящего имени на любом онлайн-сервисе, где много незнакомых людей может прочитать твою информацию. Спроси своих родителей прежде, чем сообщать кому-либо в интернете свое имя, адрес, номер телефона или любую другую персональную информацию.**
- **Дважды подумай прежде, чем разместить или рассказать о чем-нибудь в онлайн-среде. Готов ли ты рассказать об этом всем, кто находится в онлайне: твоим близким друзьям, а также посторонним людям? Помни, что, разместив информацию, фотографии или любой другой материал в сети, ты уже никогда не сможешь удалить его из интернета или помешать другим людям использовать его.**
- **Прежде чем ввести любую информацию о себе на каком-либо сайте, узнай, как может быть использована эта информация. Может ли быть опубликована вся информация или ее часть и, если «да», то где? Если ты испытываешь дискомфорт от объема запрашиваемой информации, если ты не доверяешь сайту, не давай информацию. Поищи другой похожий сервис, для работы с которым требуется меньше информации, или его администрация обещает более бережно обращаться с твоими данными.**

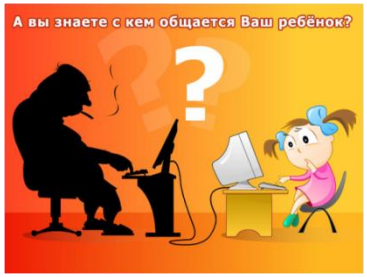
Это важно!

1. **Игнорируй плохое поведение других пользователей, уйди от неприятных разговоров или с сайтов с некорректным содержанием. Как и в реальной жизни, существуют люди, которые по разным причинам ведут себя агрессивно, оскорбительно или провокационно по отношению к другим или хотят распространить вредоносный контент. Обычно лучше всего игнорировать и затем заблокировать таких пользователей.**

2. **Не размещай ничего такого, о чем ты бы не хотел, чтобы узнали другие, чего ты бы никогда не сказал им лично.**
3. **Уважай контент других людей, который ты размещаешь или которым делишься. Например, фотография, которую тебе дал друг, является его собственностью, а не твоей. Ты можешь размещать ее в онлайн-среде только, если у тебя есть на это его разрешение, и ты должен указать, откуда ты ее взял.**
4. **Важно воздерживаться от ответа на провокационные сообщения, получаемые при помощи сообщений SMS, MMS, программ мгновенного обмена сообщениями, в электронных письмах, в чатах или во время общения в онлайн-средес другими пользователями. Вместо этого тебе нужно предпринять шаги, которые помогут исключить или ограничить попытки спровоцировать тебя.**

Если тебя запугивают в онлайновой среде:

- **Игнорируй. Не отвечай обидчику. Если он не получает ответа, ему может это наскучить и он уйдёт.**
- **Заблокируй этого человека. Это защитит тебя от просмотра сообщений конкретного пользователя.**
- **Расскажи кому-нибудь. Расскажи своей маме или папе, или другому взрослому, которому доверяешь.**
- **Сохрани доказательства. Это может быть полезным для поиска того, кто пытался тебя запугать. Сохрани в качестве доказательств тексты, электронные письма, онлайн-разговоры или голосовую почту.**



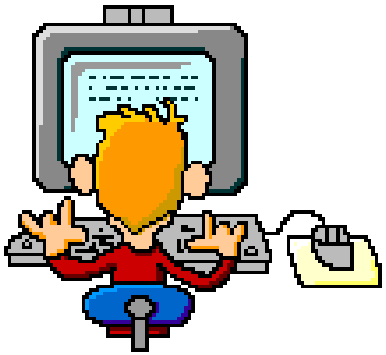
Сообщи об этом:

- **Руководству твоей школы. Образовательная организация должна иметь свою политику для ситуации с запугиванием.**
- **Твоему интернет-провайдеру, оператору мобильной связи или администратору веб-сайта. Они могут предпринять шаги, для того чтобы помочь тебе.**
- **В милицию. Если ты считаешь, что существует угроза для твоей безопасности, то кто-нибудь из взрослых, либо ты сам должен обратиться в правоохранительные органы.**

- **На линию помощи «Дети онлайн» по телефону: 88002500015 (по России звонок бесплатный) или по e-mail: helpline@online.org. Специалисты подскажут тебе, как лучше поступить**

Твои права в онлайновой среде

- **Ты имеешь права – и другие люди должны уважать их.**
- **Ты никогда не должен терпеть преследования или запугивания со стороны других людей.**
- **Законы реальной жизни также действуют и в онлайн-среде.**
- **Ты имеешь право использовать современные технологии для развития своей индивидуальности и расширения твоих возможностей.**
- **Ты имеешь право защитить свою персональную информацию.**



Твои права в онлайновой среде

- **Ты имеешь право на доступ к информации и сервисам, соответствующим твоему возрасту и личным желаниям.**
- **Ты имеешь право свободно выражать себя и право на уважение к себе, и, в то же время, должен всегда уважать других.**
- **Ты можешь свободно обсуждать и критиковать все, что опубликовано или доступно в сети.**
- **Ты имеешь право сказать НЕТ, тому, кто в онлайн-среде просит тебя о чем-то, что заставляет тебя чувствовать дискомфорт.**

Дополнительные права

Закрывайте сомнительные всплывающие окна

Всплывающие окна — это небольшие окна с содержимым, побуждающим к переходу по ссылке.

Остерегайтесь мошенничества

В Интернете легко скрыть свою личность. Рекомендуется проверять личность человека, с которым происходит общение.

Никогда не разглашайте в Интернете личную информацию, за исключением людей, которым вы доверяете.

Обсуждайте использование Интернета

Большая часть материалов, доступных в Интернете, является непригодной для несовершеннолетних. Обсудите с родителями, как правильно и безопасно использовать Интернет.

Безопасное использование своего компьютера

- **Убедись, что на твоем компьютере установлены брандмауэр и антивирусное программное обеспечение. Научись их правильно использовать. Помни о том, что эти программы должны своевременно обновляться.**
- **Хорошо изучи операционную систему своего компьютера (Windows, Linux и т. д.). Знай как исправлять ошибки и делать обновления.**
- **Если на компьютере установлена программа родительского контроля, поговори со своими родителями и договорись о настройках этой программы, чтобы они соответствовали твоему возрасту и потребностям. Не пытайся взломать или обойти такую программу!**

- **Если ты получил файл, в котором ты не уверен или не знаешь, кто его отправил, НЕ открывай его. Именно так трояны и вирусы заражают твой компьютер.**
-
-

Авторское право

- **Авторским правом защищается способ реализации идеи, но не сама идея.**
- **Разрешается копирование материала из Интернета**
- **для личного использования, но присвоение авторства**
- **этого материала запрещено.**
- **Например, при использовании материала**
- **в собственной презентации необходимо указать источник.**
- **Неразрешенное использование материала может привести**
- **к административному взысканию в судебном порядке,**
- **а также иметь прочие правовые последствия.**
- **Дополнительная информация об авторском праве: http://www.copyright.ru**

Безопасное общение в Интернете

Не делайте ваши письма длиннее, чем они должны быть. У каждой мысли есть начало и конец. Да и 15-20 слов в одном предложении электронного послания – именно та норма, которую получатель e-mail, а может воспринимать в Интернете без напряжения для глаз и психики.

Довести проверку до автоматизма. Послания без знаков препинания вышли из моды, настала эпоха онлайн-справочников, электронных словарей и всесторонней проверки правописания. Ввести многократную компьютерную проверку перед отправкой в привычку

Опытные пользователи также вносят шаблонные приветствия и благодарности, которые вставляются в начало или конец каждого послания, в награду «за уделенное время». Так что даже в Интернете не стоит пренебрегать этикетом, вне зависимости о темы переписки. Ведь электронное послание лишь создается в Сети – прочитает его, все равно, живой человек.

Посылая возмущенные письма в ответ на спам, юзер, вопреки частому заблуждению, не мстит виртуальному обидчику. Напротив, поступая таким образом, пользователь подтверждает, что его электронный адрес является «живым». Что спамеру и нужно. В итоге спамовых сообщений будет приходить только больше. Поэтому, разумнее выбрать удаление и функцию игнорирования. Или использовать программное обеспечение электронной почты, чтобы мусорные сообщения удалились автоматически.

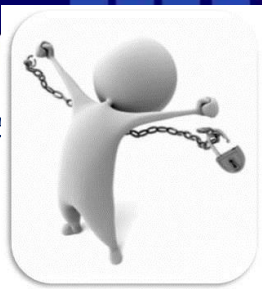
А если ответ не приходит на ум сразу? На этот случай у пользователя есть помощники: шаблоны и дежурные фразы. Этим стоит воспользоваться хотя бы по той причине, что отправитель будет традиционно терпимее к вежливой просьбе об ожидании, чем к банальному и грубому игнорированию. Есть также смысл в том, чтобы цитировать предшествующую переписку с пользователем. Такой вежливый жест поможет юзеру вспомнить все детали виртуальной беседы

Непосредственно перед отправкой, специалисты советуют всегда производить контрольное прочтение. Уверенность в том, что приложены все файлы, а в сообщении все же написано то, что запланировано значительно, сократит время в Сети при «расхлебывании» всех этих естественных и популярных ошибок в будущем.

Профилактика Интернет-зависимости у обучающихся

- **экономический аспект:** неспособность и нежелание отвлечься даже на короткое время от работы в Интернете; досада и раздражение, возникающие при вынужденных отвлечениях, и навязчивые размышления об Интернете в такие периоды; стремление проводить за работой в Интернете все увеличивающиеся отрезки времени и неспособность спланировать время окончания конкретного сеанса работы; побуждение тратить на Интернет все больше денег, не останавливаясь перед влезанием в долги;
- **межличностный аспект:** готовность лгать друзьям и членам семьи, преуменьшая длительность и частоту работы в Интернете, способность и склонность забывать при работе в Интернете о домашних делах и учебе, важных личных встречах, пренебрегая занятиями; стремление и способность освободиться на время работы в Интернете от ранее возникнувших чувств вины или беспомощности, от состояний тревоги или депрессии, обретение ощущения эмоционального подъема и своеобразной эйфории; нежелание принимать критику подобного рода образа жизни; готовность мириться с потерей друзей и круга общения из-за поглощенности работой в Интернете;
- **аспект здоровья:** резкое сокращение длительности сна; избегание физической активности, пренебрежение личной гигиеной; постоянное забывание о еде.
- За проявлениями зависимости от Интернета нередко скрываются другие **аддикции, либо психические отклонения.**
- **Расширение симптоматики**, преувеличение количества потенциальных пациентов, шумиха в прессе удобны на данный момент специалистам по психическому здоровью и исследователям этого феномена.

Преодоление Интернет-зависимости



- 1. **Признайте** свою зависимость. «Патологическое использование компьюте можно распознать по «симптомам» навязчивой потребности, пропущенным урокам и встречам, забытой и несделанной домашней работе, потере контакта с друзьями и родственниками.
- 2. **Определите проблемы,** лежащие в основе зависимости. В зависимости от возраста человека, такие моменты, ,как неуверенность в будущем, трудность успевать в школе или проблемы социальных отношений, могут подвигнуть на побег в гостеприимные виртуальные миры.
- 3. **Решайте реальные проблемы**. Стараясь избежать стрессовых ситуаций, мы только усложняем их. Вы можете найти репетитора, который поможет с домашним заданием, поможет начать решать социальные трудности, написать о том, что вас «гложет», или даже обратиться к специалисту.
- 4. **Контролируйте работу на компьютере**. Совсем не обязательно полностью выключать его — можно просто ограничить время нахождения в Интернете. В зависимости от возраста родители или сам учащийся могут взять на себя эту ответственность. Все виды деятельности должны быть выстроены по их приоритетности. Общение в Интернете не должно происходить до выполнения домашней работы или других обязанностей.
- 5. **Проводите различие** между интерактивной фантазией и полезным использованием Интернета.

Десять правил безопасности для детей в Интернете*

1. Посещайте сеть вместе с детьми, поощряйте их делиться опытом использования Интернета
2. Научите детей доверять интуиции - если их в Интернете что-либо беспокоит, пусть сообщают вам
3. Помогите ребенку зарегистрироваться в программах, требующих регистрационного имени и заполнения форм, не используя личной информации (имя ребенка, адрес электронной почты, номер телефона, домашний адрес). Для этого можно завести специальный адрес электронной почты
4. Настаивайте, чтобы дети никогда не давали своего адреса, номера телефона или другой личной информации, например, места учебы или любимого места для прогулки
5. Объясните детям, что в Интернете и реальной жизни разница между правильным и неправильным одинакова

6. Детям никогда не следует встречаться с друзьями из Интернета, так как эти люди могут оказаться совсем не теми, за кого себя выдают
7. Скажите детям, что далеко не все, что они читают или видят в Интернете, - правда, приучите их спрашивать вас, если они не уверены
8. Контролируйте действия детей с помощью современных программ, которые отфильтруют вредное содержимое, помогут выяснить, какие сайты посещает ребенок и что он там делает

9. Настаивайте, чтобы дети уважали чужую собственность, расскажите, что незаконное копирование музыки, компьютерных игр и других программ - кража
10. Научите детей уважать других, убедитесь, что они знают о том, что правила хорошего тона действуют везде - даже в виртуальном мире