ОБЩИЕ РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОМУ ИСПОЛЬЗОВАНИЮ ИНТЕРНЕТА И МОБИЛЬНОЙ СВЯЗИ

Чтобы не попадать в интернете в неприятные ситуации и не стать жертвой мошенников, ты должен соблюдать простые правила интернет-безопасности каждый раз, когда ты выходишь в сеть.

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.

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.

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.

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: 8−800−25−000−15 (по России звонок бесплатный) или по e-mail: helpline@detionline.org. Специалисты посоветуют тебе, как поступить.

Интернет-этикет

Когда общаешься в онлайне, относись к другим людям так, как ты хотел бы, чтобы относились к тебе. Избегай сквернословия и не говори вещей, которые заставят кого-то плохо себя чувствовать.

Научись "сетевому этикету", когда находишься в онлайне. Что считается делать и говорить хорошо, а что нет? Например, если ты печатаешь сообщение ЗАГЛАВНЫМИ БУКВАМИ, твой собеседник может подумать, что ты кричишь на него.

Если кто-то говорит что-то грубое или что-то неприятное - не отвечай. Уйди из чата или форума незамедлительно.

«Подозрительные» сайты

Если веб-сайт выглядит подозрительно или имеет страницу с предупреждением для лиц моложе 18 лет, покинь его немедленно. Некоторые сайты не предназначены для детей. Не заходи на неприличные сайты и не делись ссылками на такие сайты. Если ты видишь, что что-то тебя беспокоит, обсуди это с родителями или с кем-то, кому ты доверяешь. Знай, как уйти с веб-сайта, если поиск по интернету приведет тебя на неприятный или неприличный веб-сайт. Нажми control-alt-delete, если сайт не позволяет тебе выйти, или

выключи монитор компьютера и сообщи об этом взрослым.
Проверь с родителями, настроен ли твой поисковый механизм так, чтобы он блокировал материалы, предназначенные для взрослых.
Попроси родителей установить программное обеспечение для фильтрации информации из интернета, которое блокировало бы "неправильные" сайты.
Попроси родителей помочь тебе найти безопасные и забавные сайты и сделай на них "закладки" для последующего использования.

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.

РЕКОМЕНДАЦИИ ПО ПОЛЬЗОВАНИЮ СОЦИАЛЬНЫМИ СЕТЯМИ И ОНЛАЙН-ИГРАМИ

В интернете ты можешь найти много интересного, играть в игры, общаться со свертниками и встретить новых друзей. Ты имеешь право пользоваться сетью и изучить все, что может предложить тебе цифровой мир!

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.
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.

Принятие приглашений/дружбы

Большинство людей, с которыми ты общаешься в онлайн-среде, вероятно, уже являются твоими друзьями в реальной жизни. Ты также можешь установить контакт с друзьями твоих друзей. Очень часто это может быть забавным, однако готов ли ты действительно считать "другом" и поделиться информацией с фактически незнакомым тебе человеком, так же как ты делишься со своими лучшими друзьями?

В сети ты можешь общаться с людьми, ранее тебе неизвестными. Ты можешь получать просьбы от незнакомцев, которые хотели бы, чтобы ты включил их в твой список контактов и иметь возможность видеть твой профиль, но тебе не обязательно принимать их. Нет ничего плохого в том, чтобы отклонить приглашения, если ты в них не уверен. Получение большего количества контактов не является целью общения в социальной сети.

Это важно!

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.

Не размещай ничего такого, о чем ты бы не хотел, чтобы узнали другие, чего ты бы никогда не сказал им лично.

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.

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-среде с другими пользователями. Вместо этого тебе нужно предпринять шаги, которые помогут исключить или ограничить попытки спровоцировать тебя. Например:

1) многие игры позволяют исключать неприятных или нежелательных игроков;
2) очень часто можно сохранить оскорбительный текст из чата и отправить его модератору или администрации сайта;
3) большинство программ электронной почты позволяют включать фильтры для блокировки нежелательных входящих электронных писем.

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. Образовательное учреждение должно 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, токто-

нибудь из взрослых, либо ты сам должен обратиться в правоохранительные органы.
На линию помощи «Дети онлайн» по телефону: 8−800−25−000−15 (по России звонок бесплатный) или по e-mail: helpline@online.org. Специалисты подскажут тебе, как лучше поступить.

Игра в онлайновые игры

Если другой игрок ведет себя неприлично или заставляет тебя чувствовать дискомфорт, заблокируй его в своем списке игроков. Ты также можешь сообщить о нем модератору игры.
Ограничь свое игровое время, для того чтобы ты смог сделать другие вещи, такие как домашние задания, работу по дому.
Храни персональную информацию в тайне.
Не забудь выделить время для реальной жизни, для твоих друзей, занятий спортом и другой интересной деятельности.

РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОМУ ПОЛЬЗОВАНИЮ КОМПЬЮТЕРОМ

Познай свой компьютер и то, как с ним работать, чтобы ты мог правильно действовать в любой ситуации.

Научись безопасно использовать свой компьютер

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.

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 информицию.
Ты имеешь право на доступ к информации и сервисам, соответствующим твоему возрасту и личным желаниям.
Ты имеешь право свободно выражать себя и право науважение 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.

Линия помощи «Дети онлайн»

Если тебя оскорбляют и преследуют в интернете;
если тебе делают неприличные предложения в интернете;
Если ты стал жертвой сетевых мошенников;
Если ты столкнулся с опасностью во время пользования сетью интернет или мобильной связью;

Обратись на линию помощи «Дети онлайн». Тебя выслушают и помогут.
Звони по телефону 8−800−25−000−15 (звонок по России бесплатный, прием звонков осуществляется по рабочим дням с 9−00 до 18−00 мск)
Или пиши по адресу: helpline@detionline.org
Подробнее о Линии помощи ты можешь узнать на сайте www.detionline.org.

СОВЕТЫ РОДИТЕЛЯМ БЕЗОПАСНОГО ОБРАЩЕНИЯ С ТЕЛЕФОНОМ ДЕТЕЙ

Научите ребенка:
1. Правила безопасного обращения с телефоном, чтобы он не привлекал внимание уличных грабителей
Запомнить наизусть контактные телефоны родителей.
Выключать звуковой сигнал на телефоне перед выходом из квартиры / из школы, можно установить вибровызов, чтобы не пропускать вызовы.
Держать телефон или глубоко в портфеле, или в потайном кармане одежды, пользоваться шнурком для крепления к одежде.
Не отдавать телефонный аппарат в чужие руки (в том числе одноклассникам) даже на короткий промежуток времени.
Тщательно выбирать маршрут и говорить по телефону на улице и в людных местах лишь в экстренных случаях, заходя для этого в хорошо охраняемое помещение – банк, поликлинику, магазин и т.д.
Если на телефон обратили внимание потенциальные грабители, оставаться в охраняемом помещении и по телефону сообщить об этом родителям.
При попытке грабежа отдать телефон и сообщить родителям / учителям.
2. Правила разговора по телефону с незнакомыми людьми
Отвечая на звонок, не называть своего имени и имени звонящего (ребенок может ошибиться, и злоумышленники воспользуются этим, чтобы сбить его с толку).
Никогда и никому не говорить, что он дома один.
Не называть свой адрес проживания, номер школы, номер домашнего стационарного телефона.
Многие злоумышленники – хорошие психологи и способны разговорить даже взрослого, не говоря уже о ребенке. Поэтому специалисты рекомендуют пресекать разговор с незнакомцами на 5-й секунде.
Если разговор начинает приобретать неприятный характер, прекратить его и обязательно рассказать родителям о его содержании.
Не перезванивать на незнакомые номера.
Во избежание попыток злоумышленников представиться ребенку его родными звонки ребенку должны поступать ему с известных (сохраненных в адресной книжке его телефона) номеров.
3. Правила отправки SMS и MMS-сообщений
Не отвечать на сообщения, поступающие с незнакомых номеров.
Не отправлять без ведома родителей SMS на короткие номера, не участвовать в викторинах.
4. Правила безопасного использования сети Интернет
Не размещать на Интернет-ресурсах свой адрес проживания, номер школы, номер мобильного и домашнего стационарного телефонов, адрес электронной почты.
Не отправлять свои фотографии и членов своей семьи незнакомым людям, а также видео изображения.
Не открывать и не отвечать на спам и на любые письма, пришедшие с незнакомых адресов.
Прежде чем общаться с «виртуальными» незнакомцами, советоваться с родителями.
Не встречаться без ведома родителей со знакомыми по переписке в Интернете. Помнить,

что виртуальные знакомые могут оказаться не теми, за кого они себя пытаются выдавать.
Не стесняться спрашивать родителей о незнакомых вещах в Интернете.
«Используйте услуги «Родительский контроль» и «Детский интернет»
1. На телефоне
Услуга бесплатно предоставляется абонентам тарифного плана «Ринг-Динг», разработанного специально для детей и подростков.
«Родительский контроль» — это своего рода фильтр, через который проходят все Интернет-запросы с телефона ребёнка.
Этот фильтр не позволит зайти на страницы из «чёрного списка» Интернет-ресурсов: доступ к нежелательному и вредному для ребёнка содержимому будет заблокирован сервером.
2. На компьютере
Используйте специальный тариф со встроенным фильтром «Детский Интернет +» (приобретается в комплекте с модемом). При установлении Интернет-соединения с мобильного телефона все запросы проходят фильтрацию через специальный сервер с белым списком ресурсов.
Подключитесь к услуге «Антивирус Dr.Web», тарифный пакет Dr.Web Премиум. Модуль Родительского контроля, входящий в тарифный пакет Dr.Web Премиум, позволяет эффективно ограничить доступ ребенка к опасным ресурсам сети Интернет.
Тематические черные списки этого компонента не позволят посещать сайты, связанные с порнографией, насилием, наркотиками, призывами к терроризму и экстремизму, а также ограничат доступ к социальным сетям и азартным играм.
Кроме того, предусмотрена возможность самостоятельно создать список запрещенных сайтов и файлов на компьютере.
Советы по безопасности для детей
разного возраста
Дети в возрасте 5-6 лет.
Для детей такого возраста характерен положительный взгляд на мир. Они гордятся своим умением читать и считать, а также любят делиться своими идеями.
Несмотря на то, что дети в этом возрасте очень способны в использовании игр и работе с мышью, все же они сильно зависят от родителей при поиске детских сайтов.
Необходимо помочь детям делать это безопасно:
в таком возрасте желательно работать в Интернет только в присутствии родителей;
обязательно объяснить ребенку, что общение в Интернет – это не реальная жизнь, а своего рода игра. При этом постараться направить его усилия на познание мира;
добавить детские сайты в раздел Избранное. Создать там папку для сайтов, которые посещают дети;
использовать специальные детские поисковые машины, типа Quintura Kids – первая визуальная поисковая система для детей с простым интуитивным интерфейсом (http://kids.quintura.ru/);
использовать средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю;
научить ребенка никогда не выдавать в Интернет информацию о себе и своей семье;
приучить ребенка сообщать взрослым о любых угрозах или тревогах, связанных с Интернет.
Дети в возрасте от 7 до 8 лет.
Как считают психологи, для детей этого возраста абсолютно естественно желание выяснить, что они могут себе позволить делать без разрешения родителей.
В результате, находясь в Интернете ребенок будет пытаться посетить те или иные сайты, а возможно и чаты, разрешение на посещение которых он не получил бы от родителей.
Поэтому в данном возрасте особенно полезны будут те отчеты, которые предоставлены в Родительском контроле или то, что можно увидеть во временных файлах Интернет (папки

C:\Documents and Settings\Дмитрий\Local Settings\Temporary Internet Files в операционной системе Windows XP; c: \Users\User\AppData\Local\Microsoft\Windows \Temporary Internet Files в операционной системе Windows Vista).
В результате, у ребенка не будет ощущения, что ему глядят через плечо на экран, однако, родители будут знать, какие сайты посещает ребенок.
Дети в данном возрасте обладают сильным чувством семьи, они доверчивы и не сомневаются в авторитетах. Они любят играть в сетевые игры и путешествовать по Интернет. Вполне возможно, что они используют электронную почту и могут заходить на сайты и чаты, не рекомендованные родителями. В данном возрасте рекомендуется не разрешать иметь свой собственный электронный почтовый ящик, а пользоваться семейным, чтобы родители могли контролировать переписку.

Дети в возрасте 9-12 лет.

В данном возрасте дети, как правило, уже наслышаны о том, какая информация существует в Интернет. Совершенно нормально, что они хотят это увидеть, прочесть, услышать. При этом нужно помнить, что доступ к нежелательным материалам можно легко заблокировать при помощи средств Родительского контроля.

Советы по безопасности в этом возрасте:

создать список домашних правил посещения Интернет при участии детей;
требовать от ребенка соблюдения временных норм нахождения за компьютером;
показать ребенку, что взрослые наблюдают за ним не потому что им это хочется, а потому что они беспокоятся о его безопасности и всегда готовы ему помочь;
компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей;
использовать средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю;
не забывать беседовать с детьми об их друзьях в Интернет;
настаивать, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернет;
позволять детям заходить только на сайты из «белого» списка, который создан вместе с ними;
приучить детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернет;
приучить детей не загружать программы без разрешения. Объяснить им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение;
создать ребенку ограниченную учетную запись для работы на компьютере;
приучить ребенка сообщать взрослым о любых угрозах или тревогах, связанных с Интернет. Напомнить детям, что они в безопасности, если сами рассказали родителям о своих угрозах или тревогах. Похвалить их и посоветовать подойти еще раз в подобных случаях.

Дети в возрасте 13-17 лет.

В данном возрасте родителям часто уже весьма сложно контролировать своих детей, так как об Интернет они уже знают значительно больше своих родителей. Тем не менее, особенно важно строго соблюдать правила Интернет – безопасности – соглашение между родителями и детьми. Кроме того, необходимо как можно чаще просматривать отчеты о деятельности детей в Интернет.
Следует обратить внимание на необходимость содержания родительских паролей (паролей администраторов) в строгом секрете и обратить внимание на строгость этих паролей.
Советы по безопасности в этом возрасте:
установить веб-фильтр родительского контроля. Веб-фильтр оценивает содержимое веб-узлов и может блокировать те из них, содержимое которых определено как

нежелательное. Включение веб-фильтра позволит значительно уменьшить число нежелательных узлов, которые смогли бы просматривать дети, но, естественно, не гарантирует стопроцентной защиты. Так как нежелательность содержимого является субъективным критерием, следовательно, фильтры смогут блокировать далеко не все содержимое, которое вы считаете нежелательным.
использовать средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
ограничить время, проводимое ребенком за компьютером. В частности, определить дни недели и разрешенные часы доступа в соответствующий день недели. Это не позволит детям входить в систему в течение определенного периода времени. Если в момент окончания разрешенного периода времени ребенок работает за компьютером, происходит автоматический выход из системы.
установить запрет на доступ детей к отдельным играм. Запрет можно устанавливать исходя из допустимой возрастной оценки, выбора типа содержимого или запрещая доступ к определенным играм.
ведение отчетов о работе ребенка за компьютером. Выбор профиля оптимального набора правил с учетом возраста, опыта и других характеристик каждой группы пользователей. Так, например, профиль Ребенок обладает максимальным набором ограничений, а в профиле Родитель ограничений нет. Удалять предустановленные профили нельзя, но можно изменять параметры профилей Ребенок и Подросток по усмотрению взрослых.

ПРАВИЛА ПОВЕДЕНИЯ ДЛЯ УЧАЩИХСЯ В СОВРЕМЕННОЙ ИНФОРМАЦИОННОЙ СРЕДЕ

Вы должны это знать:
Не желательно размещать персональную информацию в Интернете.
Персональная информация — это номер вашего мобильного телефона, адрес электронной почты, домашний адрес и фотографии вас, вашей семьи или друзей.
Если вы публикуете фото или видео в интернете — каждый может посмотреть их.
- Не отвечайте на Спам (нежелательную электронную почту).
- Не открывайте файлы, которые прислали неизвестные Вам людей. Вы не можете знать, что на самом деле содержат эти файлы – в них могут быть вирусы или фото/видео с «агрессивным» содержанием.
- Не добавляйте незнакомых людей в свой контакт лист в IM (ICQ, MSN messenger и т.д.)
Помните, что виртуальные знакомые могут быть не теми, за кого себя выдают.
- Общаясь в Интернете, будьте дружелюбны с другими. Не пишите грубых слов, читать грубости так же неприятно, как и слышать. Вы можете нечаянно обидеть человека.
- Если рядом с вами нет родственников, не встречайтесь в реальной жизни с людьми, с которыми вы познакомились в Интернете. Если ваш виртуальный друг действительно тот, за кого он себя выдает, он нормально отнесется к вашей заботе о собственной безопасности!
Никогда не поздно рассказать взрослым, если вас кто-то обидел.

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.
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.

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.
• 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.
Принятие приглашений/дружбы
• Большинство людей, с которыми ты общаешься в онлайн-среде, вероятно, уже являются твоими друзьями в реальной жизни. Ты также можешь установить контакт с друзьями твоих друзей. Очень часто это может быть забавным, однако готов ли ты действительно считать "другом" и поделиться информацией с фактически незнакомым тебе человеком, так же как ты делишься со своими лучшими друзьями?
• В сети ты можешь общаться с людьми, ранее тебе неизвестными. Ты можешь получать просьбы от незнакомцев, которые хотели бы, чтобы ты включил их в твой список контактов и иметь возможность видеть твой профиль, но тебе не обязательно принимать их. Нет ничего плохого в том, чтобы отклонить приглашения, если ты в них не уверен. Получение большего количества контактов не является целью общения в социальной сети.
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-среде с другими пользователями. Вместо этого тебе нужно предпринять шаги, которые помогут исключить или ограничить попытки спровоцировать тебя. Например:
1) многие игры позволяют исключать неприятных или нежелательных игроков;
2) очень часто можно сохранить оскорбительный текст из чата и отправить его модератору или администрации сайта;
3) большинство программ электронной почты позволяют включать фильтры для блокировки нежелательных входящих электронных писем.
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. Образовательное учреждение должно 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.
• На линию помощи «Дети онлайн» по телефону: 8−800−25−000−15 (по России звонок бесплатный) или по e-mail: helpline@online.com. Специалисты подскажут тебе, как лучше поступить.
Игра в онлайновые игры
• Если другой игрок ведет себя неприлично или заставляет тебя чувствовать дискомфорт, заблокируй его в своем списке игроков. Ты также можешь сообщить о нем модератору игры.
• Ограничь свое игровое время, для того чтобы ты смог сделать другие вещи, такие как домашние задания, работу по дому.
• Храни персональную информацию в тайне.
• Не забудь выделить время для реальной жизни, для твоих друзей, занятий спортом и другой интересной деятельности.

РЕКОМЕНДАЦИИ ДЛЯ РОДИТЕЛЕЙ ПО ОРГАНИЗАЦИИ БЕЗОПАСНОЙ РАБОТЫ В ИНТЕРНЕТ

Бурное развитие компьютерных технологий и широкое распространение сети Интернет открывает перед людьми большие возможности для общения и саморазвития. Мы понимаем, что Интернет – это не только кладезь возможностей, но и источник угроз. Сегодня количество пользователей российской сети Интернет составляет десятки миллионов людей, и немалая часть из них – дети, которые могут не знать об опасностях мировой паутины.
Мы хотим сделать Интернет максимально безопасным для подрастающих поколений. Эта

цель осуществима, если государство, представители бизнеса, правоохранительные органы и общественность объединят усилия, а родители осознают свое главенство в обеспечении безопасности детей.

Правило 1. Внимательно относитесь к действиям ваших детей в «мировой паутине»:
• Не отправляйте детей в «свободное плавание» по Интернету. Старайтесь активно участвовать в общении ребенка с Интернет, особенно на этапе освоения.
• Беседуйте с ребенком о том, что нового для себя он узнает с помощью Интернет и как вовремя предупредить угрозы.
Правило 2. Информируйте ребенка о возможностях и опасностях, которые несет в себе сеть:
• Объясните ребенку, что в Интернете как в жизни встречаются и «хорошие», и «плохие» люди. Объясните, что если ребенок столкнулся с негативом или насилием от другого пользователя Интернет, ему нужно сообщить об этом близким людям.
• Научите ребенка искать нужную ему информацию и проверять ее, в том числе с Вашей помощью.
• Научите ребенка внимательно относиться к скачиванию платной информации и получению платных услуг из Интернет, особенно путём отправки sms, – во избежание потери денег.
• Сформируйте список полезных, интересных, безопасных ресурсов, которыми может пользоваться Ваш ребенок, и посоветуйте их использовать.
Правило 3. Выберите удобную форму контроля пребывания вашего ребенка в Сети:
• Установите на Ваш компьютер необходимое программное обеспечение – решение родительского контроля, антивирус Касперского или Doctor Web.
• Если Ваш ребенок – учащийся младших классов и остается часто дома один, ограничьте время пребывания Вашего ребенка в Интернете.
• Если компьютер используется всеми членами семьи, установите его в месте, доступном для всех членов семь.