Приложение № 1
к приказу № 15
от 10.01.2022

УТВЕРЖДАЮ:
И.о. Директора МБОУ «Школа № 18»
_____ Л.В. Щукина

ПОЛОЖЕНИЕ
об информационной безопасности
МБОУ «Школа № 18»

1. Общие положении

1.1. Информационная безопасность является одним из составных элементов комплексной безопасности в МБОУ «Школа № 18» (далее - Школа), порядок организации работ по её созданию и функционированию.

1.2. Данное положение разработано в соответствии с Федеральным законом Российской Федерации от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации», п. 3 ст. 47 Трудового кодекса Российской Федерации от 30 декабря 2001 г. № 197-ФЗ (с изм. и доп.), Федеральным законом от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации", Федеральным законом от 27 июля 2006 г. № 152-ФЗ "О персональных данных" и имеет статус локального нормативного акта образовательной организации.

Если нормами действующего законодательства Российской Федерации предусмотрены иные требования, чем настоящим Положением, применяются нормы законодательства Российской Федерации.

1.3. Под информационной безопасностью Школы следует понимать состояние защищенности информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности. Система информационной безопасности направлена на предупреждение угроз, их своевременное выявление, обнаружение, локализацию или ликвидацию.

1.4. Использование сети Интернет в образовательной организации подчинено следующим принципам:

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

1.5. К объектам информационной безопасности в Школе относятся:

- информационные ресурсы, содержащие конфиденциальную информацию, представленную ввиде документированных информационных массивов и баз данных;
- информацию, защита которой предусмотрена законодательными актами РФ, в т. ч.персональные данные;
- средства и системы информатизации - средства вычислительной и организационной техники, локальной сети, общесистемное и прикладное программное обеспечение, автоматизированные системы управления рабочими местами, системы связи и передачи данных, технические средства сбора, регистрации, передачи, обработки и отображения

информации.

1.6. Система информационной безопасности (далее - СПБ) должна обязательно обеспечивать:

- конфиденциальность (защиту информации от несанкционированного раскрытия или перехвата);
- целостность (точность и полноту информации и компьютерных программ);
- доступность (возможность получения пользователями информации в пределах их компетенции).

1.7. Обеспечение информационной безопасности осуществляется по следующим направлениям:

• правовая зашита - это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;

• организационная зашита - это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба;• инженерно-техническая защита - это использование различных технических средств, препятствующих нанесению ущерба.

2. Правовые нормы обеспечения информационной безопасности.

2.1. Школа имеет право определять состав, объем и порядок защиты сведений конфиденциального характера, персональных данных обучающихся, работников Школы, требовать от своих сотрудников обеспечения сохранности и защиты этих сведений от внешних и внутренних угроз.

2.2. Школа обязана обеспечить сохранность конфиденциальной информации.

2.3. Администрация школы:

• назначает ответственного за обеспечение информационной безопасности;

• издаёт нормативные и распорядительные документы, определяющие порядок выделения сведений конфиденциального характера и механизмы их защиты;

• имеет право включать требования по обеспечению информационной безопасности в коллективный договор;

• имеет право включать требования по защите информации в договоры по всем видам деятельности;

• разрабатывает перечень сведений конфиденциального характера;

• имеет право требовать защиты интересов школы со стороны государственных и судебных инстанций.

2.4. Организационные и функциональные документы по обеспечению информационной безопасности:

• приказ директора Школы о назначении ответственного за обеспечение информационной безопасности;

• должностные обязанности ответственного за обеспечение информационной безопасности;• перечень защищаемых информационных ресурсов и баз данных;

• инструкция, определяющая порядок предоставления информации сторонним организациям по их запросам, а также по правам доступа к ней сотрудников Школы и др.

2.5.Порядок допуска сотрудников Школы к информации предусматривает:

• принятие работником обязательств о неразглашении доверенных ему сведений конфиденциального характера;

• ознакомление работника с нормами законодательства Российской Федерации и Школы об информационной безопасности и ответственности за разглашение информации конфиденциального характера;

• инструктаж работника специалистом по информационной безопасности;• контроль работника ответственным за информационную безопасность при работе с информацией конфиденциального характера.

3. Использование сети Интернет.

3.1. Использование сети Интернет в Школе осуществляется в целях образовательного процесса. В рамках развития личности, ее социализации и получения знаний в области

компьютерной грамотности лицо может осуществлять доступ к ресурсам не образовательной направленности.

3.2. ***Работники Школы вправе:***

• размещать информацию в сети Интернет на интернет - ресурсах Школы;

• иметь учетную запись электронной почты на интернет - ресурсах Школы.

3.3. ***Работникам Школы запрещено*** размещать в сети Интернет и на образовательных ресурсах информацию:

- противоречащую требованиям законодательства Российской Федерации и локальным нормативным актам Школы;

- не относящуюся к образовательному процессу и не связанную с деятельностью Школы;

- нарушающую нравственные и этические нормы, требования профессиональной этики.

3.4. ***Обучающиеся Школы вправе:***

• использовать ресурсы, размещенные в сети Интернет, в том числе интернет-ресурсы Школы, в порядке и на условиях, которые предусмотрены настоящим Положением.

• размещать информацию и сведения на интернет - ресурсах Школы.

5. ***Обучающемся запрещено:***

- находиться на ресурсах, содержание и тематика которых недопустима для несовершеннолетних и / или нарушает законодательство Российской Федерации;

- осуществлять любые сделки через интернет;

- загружать файлы на компьютер Школы без разрешения уполномоченного лица;

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

6. Запрет и снятие такого запрета на допуск пользователей к работе в сети Интернет устанавливает уполномоченное лицо, назначенное приказом директора Школы.

7. Если в процессе работы пользователем будет обнаружен ресурс, содержимое которого не совместимо с целями образовательного процесса, он обязан незамедлительно сообщить об этом уполномоченному лицу с указанием интернет - адреса (URL) и покинуть данный ресурс.

7.1. ***Уполномоченное лицо обязано:***

• принять сообщение пользователя;

• принять меры по отключению выхода на данный ресурс с интернет ресурсов Школы;

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

Передаваемая информация должна содержать: в интернет-адрес (URL) ресурса;

• тематику ресурса, предположения о нарушении ресурсом законодательства Российской Федерации либо несовместимости с задачами образовательного процесса;

• дату и время обнаружения;

• информацию об установленных в образовательной организации технических средствах ограничения доступа к информации.

4. Мероприятия по обеспечению информационной безопасности.

4.1. Для обеспечения информационной безопасности в Школе требуется проведение следующих первоочередных мероприятий:

- защита интеллектуальной собственности Школы;

- защита компьютеров, локальных сетей и сети подключения к системе Интернета;

- организация защиты конфиденциальной информации, в т. ч. персональных данных работников и обучающихся Школы;

- учет всех носителей конфиденциальной информации.

5. Организация работы с информационными ресурсами и технологиями.

5.1. Система организации делопроизводства:

• учет всей документации Школы, в т. ч. и на электронных носителях, с классификацией по сфере применения, дате, содержанию; регистрация и учет всех входящих

(исходящих) документов Школы в специальном журнале информации о дате получения (отправления) документа, откуда поступил или куда отправлен, классификация (письмо, приказ, распоряжение и т. д.);

• регистрация документов, с которых делаются копии, в специальном журнале (дата копирования, количество копий, для кого или с какой целью производится копирование);

• особый режим уничтожения документов.

5.2. В ходе использования, передачи, копирования и исполнения документов также необходимо соблюдать определенные правила:

5.2.1. Все документы, независимо от грифа, передаются исполнителю под роспись в журнале учета документов.

5.2.2. Документы, дела и издания с грифом "Для служебного пользования" ("Ограниченного пользования") должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах.

5.2.3. Выданные для работы дела и документы с грифом "Для служебного пользования" ("Ограниченного пользования") подлежат возврату в канцелярию в тот же день.

5.2.4. Передача документов исполнителю производится только через ответственного за организацию делопроизводства.

5.2.5. Запрещается выносить документы с грифом "Для служебного пользования" за пределы школы.

5.2.6. При смене работников, ответственных за учет и хранение документов, дел и изданий, составляется по произвольной форме акт приема-передачи документов.

5.3. Для организации делопроизводства приказом директора школы назначается ответственное лицо. Делопроизводство ведется на основании инструкции по организации делопроизводства, утвержденной директором школы.

Контроль за порядком его ведения возлагается на ответственного за информационную безопасность.

6. О системном администрировании и обязанностях информационную безопасность.

6.1. Задачи, связанные с мерами системного администрирования, обеспечивающего информационную безопасность, являются частью работы системного администратора МБОУ «Школа № 18».

6.2. Для решения задач информационной безопасности системный администратор обязан:

• следить за соблюдением требований по парольной защите, в том числе осуществлять изменение паролей по мере необходимости (утрата пароля, появление новых пользователей в связи с изменением кадрового состава и пр.);

• обеспечивать функционирование программно-аппаратного комплекса защиты по внешним цифровым линиям связи;

• обеспечивать мероприятия по антивирусной защите, как на уровне серверов, так и на уровне пользователей;

• обеспечивать нормальное функционирование системы резервного копирования.

7. Антивирусная защита.

7.1. Правила пользования внешними сетевыми ресурсами (Интернет, электронная почта и т.д.). Основным способом проникновения компьютерных вирусов на компьютер пользователя в настоящее время является Интернет и электронная почта. В связи с этим не допускается работа без организации антивирусной защиты. Антивирусная защита организуется посредством лицензионного антивирусного программного обеспечения.

7.2. Обновление базы используемого антивирусного программного обеспечения осуществляется автоматически не реже 1 раза в день.

7.3. За своевременное обновление антивирусного программного обеспечения отвечает системный администратор школы.

Приложение № 2
к приказу № 15
от 01.09.2022г

УТВЕРЖДАЮ:
И.о. Директора МБОУ «Школа № 18»
_____ Л.В. Щукина

Инструкция
по обеспечению информационной безопасности
при использовании сети Интернет
МБОУ «Школа № 18»

В современной школе информация, информационная инфраструктура – один из главных компонентов учебного процесса.

Информация и обеспечивающие ее системы и сети являются ценными ресурсами. Собственники информации сталкиваются с возрастающей угрозой нарушения режима безопасности, исходящей из различных источников. Информационным системам и сетям могут угрожать такие опасности, как: компьютерное мошенничество, компьютерные вирусы, хакеры, вандализм, хищение, разглашение конфиденциальной информации и другие виды угроз.

При построении системы информационной безопасности решающую роль играет организационная защита. В первую очередь необходимо учесть следующие аспекты:

1. Безопасность информации может быть обеспечена при комплексном использовании всего арсенала имеющихся средств защиты.

2. Никакая система защиты информации не может обеспечить требуемого уровня безопасности информации без соответствующей подготовки пользователей и соблюдения ими установленных правил.

3. Процесс построения системы информационной безопасности не является разовым мероприятием. Он должен постоянно совершенствоваться, быть управляемым.

Такой подход является главным стратегическим звеном во всей системе информационной безопасности, а информация – главным элементом защиты.

Следует помнить, что информация существует в различных формах.
Ее можно хранить на компьютерах, передавать по локальным сетям и через Интернет, распечатывать на бумажных носителях, копировать, сканировать, а также озвучивать в разговорах. В целях безопасности все виды носителей информации (документы, пленки, магнитные ленты, дискеты, диски и др.), используемые для ее хранения, должны быть надлежащим образом защищены.

Очень часто, рассматривая информационную безопасность, путают и отождествляют два понятия: "компьютерная безопасность" и "информационная безопасность".

Это неверно. "Компьютерная безопасность" очень важна, но она является только одной из составляющих "информационной безопасности".

Информационная безопасность – это процесс обеспечения конфиденциальности, целостности и доступности информации.

Единая информационная система в школе включает в себя:

- сайт образовательного учреждения;
- электронный журнал/электронный дневник;
- медиатеку на базе школьной библиотеки;
- официальную группу школы в «ВКонтакте»;

- компьютерное и интерактивное оборудование;
- локальную сеть школы;
- закрытые группы классных коллективов «ВКонтакте»;

Информационная безопасность в школе обеспечивает:

- целостность персональных данных — защита от сбоев, ведущих к потере информации, а также зашита от неавторизованного создания или уничтожения данных;
- конфиденциальность информации;
- доступность информации для всех авторизованных пользователей.

В образовательном учреждении принятые следующие меры по обеспечению информационной безопасности участников образовательного процесса:

- защита компьютеров от внешних несанкционированных воздействий (компьютерные вирусы, атаки хакеров и т. д.) через использование программно-технических средств антивирусной защиты компьютерной техники в образовательном учреждении и своевременное их обновление.
- заключен договор с провайдером по осуществлению контентной фильтрации трафика, ежемесячно проводится контроль фильтрации сайтов с содержимым, не соответствующим задачам образования.
- бучение детей основам информационной безопасности, воспитание информационной культуры через уроки компьютерной грамотности, классные часы, уроки безопасного поведения в сети интернет в рамках программы учебного предмета «Основы безопасности жизнедеятельности».
- систематический инструктаж педагогических работников и обучающихся по вопросам информационной безопасности с фиксацией в ведомостях инструктажей.
- ведение журнала регистрации выхода учащихся и педагогов в Интернет с фиксацией в журнале по использованию цифрового оборудования.
- ознакомление родителей с нормативно-правовой базой по защите детей от распространения вредной для них информации на родительских собраниях и на странице школьного сайта «Информационная безопасность».
- обеспечение доступа обучающихся (в библиотеке, кабинете информатики) и педагогов (в учительской) к электронным образовательным ресурсам сети Интернет.
- ежегодное участие во Всероссийской акции, посвящённой безопасности школьников в сети Интернет, проведение конкурса плакатов по информационной безопасности, мероприятия «Информационная безопасность» в рамках Недели безопасности в ОУ, классные часы, инструктажи.

Памятка
для обучающихся МБОУ «Школа № 18»
по обеспечению информационной безопасности
при использовании сети Интернет

Данная памятка по обеспечению информационной безопасности при использовании сети Интернет разработана для учащихся начального, основного, среднего уровня обучения с целью урегулирования действия обучающихся во время пользования интернет – ресурсами.

Классным руководителям необходимо ознакомить обучающихся с правилами безопасности в Интернете, провести беседу с учащимися. Приведенные правила безопасности в сети Интернет школьникам необходимо помнить и придерживать их.

1. Правила безопасности в сети Интернет для обучающихся начального уровня обучения.

✓ Всегда задавайте вопросы родителям о незнакомых вам вещах в Интернете. Они подробно расскажут, что безопасно делать, а что может причинить вред.

✓ Перед тем, как подружиться с кем-либо в сети Интернет, спросите у родителей как вести безопасное общение.

✓ Не при каких обстоятельствах не рассказывайте о себе незнакомцам. Где и с кем вы живете, в какой школе обучаетесь, номер телефона должны знать исключительно Ваши друзья и родственники.

✓ Не отсылайте свои фотографии людям, совершенно не знакомым Вам. Нельзя чтобы совершенно незнакомые люди видели Ваши фотографии, фотографии Ваших друзей или Вашей семьи.

✓ Никогда не соглашайтесь на личную встречу с людьми из Интернета без сопровождения родителей. В сети Интернет много людей рассказывающих о себе неправду.

✓ Ведя общение в Интернет сети, всегда будьте дружелюбны к другим людям. Нельзя писать грубые слова, поскольку читать грубости так же неприятно, как и слышать. Вы можете случайно обидеть человека.

✓ В случае, если вас кто-то расстроил или обидел, следует обязательно рассказать родителям.

2. Правила безопасности в сети Интернет для обучающихся основного уровня обучения.

✓ Регистрируясь на различных сайтах, всегда старайтесь не указывать личную информацию потому, что она может быть доступна совершенно незнакомым людям. Так же, не желательно размещать своё фото, давая, тем самым, представление о Вашей внешности, совершенно посторонним людям.

✓ Пользуйтесь веб-камерой исключительно для общения с друзьями. Следите, чтобы посторонние вам люди не могли видеть ваш разговор, т.к. его можно записать.

✓ Нежелательные письма от незнакомцев называются «Спам». Если вы вдруг получили подобное письмо, никогда не отвечайте на него. Если Вы ответите на такое письмо, отправивший будет знать, что вы используете свой электронный почтовый ящик и будет продолжать слать вам «Спам».

✓ В случае, если вы получили письмо с совершенно незнакомого адреса, его желательно не открывать. Такие письма зачастую содержат вирусы.

✓ Если вы получаете письма с неприятным и оскорбительным для вас содержанием или кто-нибудь ведет себя по отношению к вам неподобающим образом, обязательно сообщите об этом.

✓ Если вдруг вас кто-либо расстроил или обидел, расскажите обо всем взрослому.

3. Правила безопасности в сети Интернет для обучающихся среднего уровня обучения.

✓ Не рекомендуется размещение личной информации в Интернет сети. Личная информация: номер вашего мобильного телефона, адрес электронной почты, домашний адрес и ваши фотографии, фотографии членов вашей семьи или друзей.

✓ Если вы выложите фото или видео в интернете — любой может посмотреть их.

✓ Никогда не отвечайте на «Спам» (нежелательную электронную почту).

✓ Нельзя открывать файлы, полученные от неизвестных Вам людей. Вы ведь не знаете, что в действительности содержат эти файлы в них могут находиться вирусы или фото/видео с «агрессивным» содержимым.

✓ Никогда не добавляйте незнакомых вам людей в свой список контактов в IM (ICQ, MSN messenger и т.д.).

✓ Не забывайте, что виртуальные друзья и знакомые могут быть не теми на самом деле, за кого себя выдают.

✓ Если около вас или поблизости с вами нет родственников, никогда не встречайтесь в реальности с людьми, с которыми вы познакомились в Интерне сети. Если ваш виртуальный друг в действительности тот, за кого себя выдает, он с пониманием отнесется к вашей заботе о собственной безопасности!

✓ В любое время можно рассказать взрослым, если вас кто-либо обидел.

Памятка для родителей
по обеспечению информационной безопасности
при использовании сети Интернет

Определение термина "информационная безопасность детей" содержится в Федеральном законе № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию", регулирующими отношения, связанные с защитой детей от информации, причиняющей вред их здоровью и (или) развитию.

Согласно данному закону "информационная безопасность детей" - это состояние защищенности, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию.

В силу Федерального закона № 436-ФЗ информацией, причиняющей вред здоровью и (или) развитию детей, является:

- информация, запрещенная для распространения среди детей;
- информация, распространение которой ограничено среди детей определенных возрастных категорий.

К информации, запрещенной для распространения среди детей, относится:

✓ информация, побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в т.ч. причинению вреда своему здоровью, самоубийству;

✓ способность вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе; принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;

✓ обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям и животным;

✓ отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;

✓ оправдывающая противоправное поведение;

✓ содержащая нецензурную брань;

✓ содержащая информацию порнографического характера.

К информации, распространение которой ограничено среди детей определенного возраста, относится:

✓ информация, представляемая в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия;

✓ вызывающая у детей страх, ужас или панику, в т.ч. представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий;

✓ представляемая в виде изображения или описания половых отношений между мужчиной и женщиной;

✓ содержащая бранные слова и выражения, не относящиеся к нецензурной брани.

С учетом этого Вам предлагаются правила работы в сети Интернет для различных возрастных категорий, соблюдение которых позволит обеспечить информационную безопасность ваших детей.

Общие правила для родителей

1. Независимо от возраста ребенка используйте программное обеспечение, помогающее фильтровать и контролировать информацию, но не полагайтесь полностью на него. Ваше внимание к ребенку - главный метод защиты.

2. Если Ваш ребенок имеет аккаунт на одном из социальных сервисов (LiveJoumal, blogs.mail.ru, vkontakte.ru и т.п.), внимательно изучите, какую информацию помещают его участники в своих профилях и блогах, включая фотографии и видео.

3. Проверьте, с какими другими сайтами связан социальный сервис Вашего ребенка. Странички Вашего ребенка могут быть безопасными, но могут и содержать ссылки на нежелательные и опасные сайты (например, порносайт, или сайт, на котором друг упоминает номер сотового телефона Вашего ребенка или Ваш домашний адрес)

4. Поощряйте Ваших детей сообщать обо всем странном или отталкивающем и не слишком остро реагируйте, когда они это делают (из-за опасения потерять доступ к Интернету дети не говорят родителям о проблемах, а также могут начать использовать Интернет вне дома и школы).

5. Будьте в курсе сетевой жизни Вашего ребенка. Интересуйтесь, кто их друзья в Интернет так же, как интересуетесь реальными друзьями.

Возраст детей от 13 до 17 лет.

В этом возрасте подростки активно используют поисковые машины, пользуются электронной почтой, службами мгновенного обмена сообщениями, скачивают музыку и фильмы. Мальчикам в этом возрасте больше по нраву сметать все ограничения, они жаждут грубого юмора, азартных игр, картинок "для взрослых". Девочки предпочитают общаться в чатах, при этом они гораздо более чувствительны к сексуальным домогательствам в Интернете.

Зачастую в данном возрасте родителям уже весьма сложно контролировать своих детей, так как об Интернете они уже знают значительно больше своих родителей. Тем не менее, не отпускайте детей в "свободное плавание" по Интернету. Старайтесь активно участвовать в общении ребенка в Интернете.

Важно по-прежнему строго соблюдать правила Интернет - безопасности - соглашение между родителями и детьми.

Кроме того, необходимо как можно чаще просматривать отчеты о деятельности детей в Интернете. 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 от 13 до 17 лет:

1. Создайте список домашних правил посещения Интернета при участии подростков и требуйте безусловного его выполнения. Обговорите с ребенком список запрещенных сайтов ("черный список"), часы работы в Интернете, руководство по общению в Интернете (в том числе в чатах).

2. Компьютер с подключением к сети Интернет должен находиться в общей комнате.

3. Не забывайте беседовать с детьми об их друзьях в Интернете, о том, чем они заняты таким образом, будто речь идет о друзьях в реальной жизни. Спрашивайте о людях, с

которыми дети общаются посредством служб мгновенного обмена сообщениями, чтобы убедиться, что эти люди им знакомы.

4. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.

5. Необходимо знать, какими чатами пользуются Ваши дети. Поощряйте использование модерируемых чатов и настаивайте, чтобы дети не общались в приватном режиме.

6. Настаивайте на том, чтобы дети никогда не встречались лично с друзьями из сети Интернет.

7. Приучите детей не выдавать свою личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернете.

8. Приучите детей не загружать программы без Вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.

9. Приучите Вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Напомните детям, что они в безопасности, если сами рассказали вам, о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

10. Расскажите детям о порнографии в Интернете. Помогите им защититься от спама. Научите подростков не выдавать в Интернете своего реального электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.

11. Приучите себя знакомиться с сайтами, которые посещают подростки.

12. Научите детей уважать других в интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде - даже в виртуальном мире.

13. Объясните детям, что ни в коем случае нельзя использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.

14. Обсудите с подростками проблемы сетевых азартных игр и их возможный риск. Напомните, что дети не могут играть в эти игры согласно закону. Постоянно контролируйте использование Интернета Вашим ребенком! Это не нарушение его личного пространства, а мера предосторожности и проявление Вашей родительской ответственности и заботы.