Родительское собрание на тему:

«Информационная безопасность и психологическая защита детей».

10 правил безопасной работы в Интернете для детей.

Прежде чем позволять своим детям выходить в Интернет без вашего контроля, составьте вместе с ними правила, которых они должны будут придерживаться.

Если вы не знаете с чего начать, ознакомьтесь с приведенными ниже советами, которые помогут вам научить детей принципам безопасной работы в Интернете.

1.

Убедите своих детей делиться с вами впечатлениями от работы в Интернете. Путешествуйте в Интернете вместе с детьми.

2.

Научите детей доверять интуиции. Если что-нибудь в Интернете будет вызывать у них психологический дискомфорт, пусть дети рассказывают вам об этом.

3.

Если ваши дети общаются в чатах, пользуются [программами мгновенной передачи сообщений](https://infourok.ru/go.html?href=http%3A%2F%2Fwww.microsoft.com%2Fprotect%2Fproducts%2Fcomputer%2Fimsafety.mspx), играют в сетевые игры или занимаются в Интернете чем-то другим, что требует указания идентификационного имени пользователя, помогите им выбрать это имя и убедитесь в том, что оно не содержит никакой личной информации.

4.

Запретите своим детям сообщать другим пользователям Интернета адрес, номер телефона и другую личную информацию, в том числе номер школы и любимые места для игр.

5.

Объясните детям, что нравственные принципы в Интернете и реальной жизни одинаковы.

6.

Научите детей уважать других пользователей Интернета. Разъясните детям, что при переходе в виртуальный мир нормы поведения нисколько не изменяются.

7.

Добейтесь от детей уважения к собственности других пользователей Интернета. Расскажите детям, что незаконное копирование продуктов труда других людей, в том числе музыки, видеоигр и других программ, почти не отличается от воровства в магазине.

8.

Убедите детей в том, что они не должны встречаться с интернет-друзьями лично. Скажите, что интернет-друзья могут на самом деле быть не теми, за кого они себя выдают.

9.

Объясните детям, что верить всему, что они видят или читают в Интернете, нельзя. Скажите им, что при наличии сомнений в правдивости какой-то информации им следует обратиться за советом к вам.

10.

Контролируйте действия своих детей в Интернете с помощью специализированного программного обеспечения. Средства родительского контроля помогают блокировать вредные материалы, следить за тем, какие веб-узлы посещают ваши дети, и узнавать, что они там делают.

Повышение уровня безопасности детей при посещении ими веб-узлов социальных сетей

При взгляде на ребенка, делающего домашнее задание за семейным компьютером в гостиной или общающегося и просматривающего страницы в Интернете через сотовый телефон на заднем сиденье машины, может показаться, что он постоянно находится в Сети.

Социальные веб-узлы крайне популярны у подростков и набирают все большую популярность среди детей младшего возраста. Дети используют веб-узлы социальных сетей для общения как с детьми из других частей мира, так и с теми, кого каждый день встречают в школе. На веб-узлах социальных сетей дети выражают свои чувства, а иногда даже ищут сведения о ком-то, кого им довелось повстречать на вечеринке или в школе. Например, после личной встречи ребенок может посетить веб-узел своего нового знакомого, чтобы лучше понять, хочет ли он с ним подружиться.

Сегодня многие дети не видят большой разницы между жизнью в реальном мире и в Интернете. Они посещают как социальные веб-узлы, созданные специально для детей (например, Webkinz или Club Penguin), так и веб-узлы, предназначенные для взрослых (например, Windows Live Spaces, YouTube, MySpace, Flickr, Twitter, Facebook и другие). Что бы они ни делали, они должны понимать, что многие такие веб-страницы может увидеть любой человек, имеющий доступ в Интернет.

На эти веб-узлах дети

общаются;

•

играют в игры;

•

размещают свои фотографии и видеоролики и смотрят чужие;

•

ведут блоги;

•

публикуют данные о себе.

К сожалению, некоторые сведения, размещаемые детьми на своих страницах, могут сделать их объектом [фишинг-афер](https://infourok.ru/go.html?href=http%3A%2F%2Fwww.microsoft.com%2Frus%2Fprotect%2Fyourself%2Fphishing%2Fidentify.mspx), запугивания и действий интернет-преступников. Ниже описано несколько способов, которые позволяют сделать использование веб-узлов социальных сетей более безопасным для ребенка.

Обсуждайте с детьми их опыт использования веб-узлов. Просите детей рассказывать вам, если что-либо, с чем они столкнулись на этих веб-узлах, пугает их или вызывает у них дискомфорт. Ведите себя спокойно и напоминайте детям, что они могут без опасений рассказывать вам обо всем. Объясните, что готовы помочь им разрешить любую ситуацию благоприятным образом.

•

Установите правила пользования Интернетом дома По мере того как дети начинают самостоятельно пользоваться Интернетом, имеет смысл составить список правил его использования, который бы их устроил. В этих правилах должно быть указано, разрешается ли ребенку посещать веб-узлы социальных сетей и на каких условиях. Дополнительные сведения о выработке правил см. в статье [Использование семейных договоров для обеспечения безопасности детей в Интернете](https://infourok.ru/go.html?href=http%3A%2F%2Fwww.microsoft.com%2Frus%2Fprotect%2Ffamily%2Fguidelines%2Fcontract.mspx).

•

Убедитесь, что ваши дети следуют ограничениям по возрасту, установленным на веб-узле.Рекомендуемый возраст регистрации на веб-узлах социальных сетей — 13 лет и старше. Если ваши дети младше рекомендуемого возраста, не позволяйте им посещать эти веб-узлы. Помните, что сами службы могут не препятствовать регистрации малолетних детей на веб-узле.

•

Изучите веб-узел сами. Просмотрите сайты, которые собирается посещать ваш ребенок, и убедитесь, что и вы, и ребенок понимаете суть политики конфиденциальности и кодекса поведения. Выясните, отслеживается ли на сайте размещаемое его пользователями содержимое. Кроме того, периодически просматривайте страницу своего ребенка. Другие советы см. в статье [Советы по безопасному ведению блога для родителей и детей](https://infourok.ru/go.html?href=http%3A%2F%2Fwww.microsoft.com%2Frus%2Fprotect%2Ffamily%2Factivities%2Fblogging.mspx).

•

Запретите детям лично встречаться с теми, с кем они общались исключительно в Сети, убедите их общаться только с людьми, которых они знают лично. Дети могут подвергнуться серьезной опасности при личной встрече с людьми, с которыми они общались исключительно в Интернете. Чтобы защитить своих детей от этой опасности, убедите их использовать такие веб-узлы для общения только со своими друзьями, а не с незнакомыми людьми.

Может оказаться недостаточным просто запретить ребенку общаться с незнакомыми людьми, потому что он может не считать незнакомым человека, с которым «познакомился» в Сети. Другие советы по обеспечению безопасности детей в Интернете см. в статье[Интернет-преступники: как свести риск к минимуму](https://infourok.ru/go.html?href=http%3A%2F%2Fwww.microsoft.com%2Frus%2Fprotect%2Ffamily%2Fguidelines%2Fpredators.mspx).

•

Убедитесь в том, что ваши дети не используют полные имена. Пусть ребенок использует только имя или псевдоним, который не будет привлекать излишнего внимания. Также запретите детям использовать полные имена своих друзей.

•

Контролируйте размещение любых других личных данных в профиле ребенка. Многие веб-узлы социальных сетей позволяют детям входить в общие группы, которые объединяют учащихся одной школы.

Внимательно относитесь к ситуациям, когда дети размещают такие данные или другие сведения о себе, с помощью которых можно выяснить их личность (например, эмблему своей школы, фотографию рабочего места или название города, в котором они живут). Излишняя открытость может сделать ребенка объектом запугивания, мошенничества, действий интернет-преступников или кражи личных сведений. Дополнительные сведения см. в статье [Распознавание фишинг-афер и мошеннических сообщений электронной почты](https://infourok.ru/go.html?href=http%3A%2F%2Fwww.microsoft.com%2Frus%2Fprotect%2Fyourself%2Fphishing%2Fidentify.mspx).

•

Рассмотрите возможность использования веб-узла с ограничением доступа. Некоторые веб-узлы социальных сетей позволяют защищать свою страницу с помощью пароля или реализуют другие методы защиты, разрешая просмотр сведений о детях только тем, кого они знают. Например, служба MSN Spaces позволяет указать, кому разрешается просматривать веб-узел, начиная от всех пользователей Интернета и заканчивая только выбранными людьми.

•

Обращайте внимание на детали фотографий. Объясните ребенку, что по фотографиям можно многое узнать о человеке. Убедите детей не размещать свои фотографии или фотографии друзей с легко узнаваемыми деталями, такими как названия улиц, номера машин или название школы на одежде.

•

Предупредите ребенка, что нельзя показывать свои чувства незнакомым людям. Наверное, вы уже сказали детям, что не следует общаться с незнакомцами в сети. Однако дети используют веб-узлы социальных сетей, чтобы вести дневники и писать стихотворения, в которых часто весьма открыто выражают свои чувства.

Объясните детям, что их записи может прочитать кто угодно, у кого есть доступ к Интернету, и что интернет-преступники охотятся на эмоционально ранимых детей. Дополнительные сведения см. в статье [Десять правил безопасной работы в Интернете для детей](https://infourok.ru/go.html?href=http%3A%2F%2Fwww.microsoft.com%2Frus%2Fprotect%2Ffamily%2Fguidelines%2Frules.mspx).

•

Расскажите детям о запугивании с помощью Интернета. Как только дети достаточно повзрослеют для посещения веб-узлов социальных сетей, расскажите им о практике запугивания в Интернете. Объясните ребенку, что если ему кажется, что его запугивают, следует сказать об этом родителям, учителю или кому-то из взрослых, кому он доверяет. Кроме того, нужно пояснить ребенку, что общаться с другими людьми в Интернете надо так же, как он общался бы с ними вживую. Попросите детей вести себя с другими людьми так же, как они хотели бы, чтобы себя с ними вели другие.

•

Удаление страницы ребенка. Если ребенок отказывается подчиняться установленным вами правилам, призванным его защитить, то после попытки на него повлиять можно связаться с администрацией веб-узла социальной сети, которую посещает ребенок, и попросить удалить его страницу. Кроме того, можно попробовать воспользоваться средствами фильтрации содержимого в Интернете (такими как [семейная безопасность Windows Live OneCare (EN)](https://infourok.ru/go.html?href=%234)) в качестве дополнения (но не замены) родительского контроля.