7. Специальные программы для родителей

Существуют различные программы, которые ограничивают доступ к подозрительным сайтам, помогают контролировать действия и безопасность детей в Сети и лимитируют время пребывания в интернете. Можно ограничить доступ к социальным сетям, видеохостингам и другим платформам в часы занятий. Так ребёнок точно не станет отлынивать от просмотра уроков.

Существуют разные специальные программы родительского контроля для обеспечения безопасности ребенка в Интернете, например, российская программа «Kaspersky Safe Kids». Данная программа представлена широким функционалом, имеет платный и бесплатный контент. Она может быть установлена как на персональный компьютер, так и на смартфон ребенка. С помощью нее родитель сможет ограничивать и блокировать нежелательный контент; просмотреть историю запросов в сети; наблюдать за экранным временем; узнать местонахождение ребёнка по GPS и др.

Основные правила безопасного поведения в Интернете для детей и родителей:

- Никому не передавать свои пароли и не перечислять денежные средства;
- Без необходимости не регистрироваться на сайтах, где нужно указывать свои персональные данные;
- Не использовать один пароль для нескольких сайтов. Использовать сложные и надежные пароли;
- По возможности использовать двухфакторную аутентификацию (когда Ваша система безопасности использует два фактора, например пароль и смс оповещение на телефон или другие меры безопасности;
- Проверять URL (название сайта, отображаемое в строке браузера, куда вы хотите зайти) перед совершением каких-либо действий на сайте;
- Не указывать в социальных сетях номер телефона, электронную почту, паспортные данные, адрес и другую информацию о себе;
- Не скачивать подозрительные файлы, не переходить по неизвестным ссылкам;
- Регулярно проверять компьютер на предмет безопасности с помощью специализированных антивирусных программ;
- Проверять, с кем Вы общаетесь в сети, не отвечать на сообщения от неизвестных пользователей без контроля со стороны родителей.

Буклет подготовлен в рамках проекта «Безопасное детство — лучшие практики» Благотворительного фонда «Дорога к дому» компании «Северсталь», реализуемого на базе Фонда поддержки социальных проектов и инициатив «Добрый город» в сотрудничестве с АНО «Ресурсный центр поддержки некоммерческих организаций и гражданских инициатив» и ЯрГУ им. П. Г. Демидова.

Отпечатано: ИП Дурынин В.В.
г. Ярославль, проспект Машиностроителей, д. 83, оф.110
ИНН 760300624335
Тираж 500 экз. 2022 г.

Безопасный Интернет для детей: полезные рекомендации

Северсталь

Добрый город

Дорога к дому

Современные интернет-технологии и разнообразные онлайн-приложения содержат в себе спектр возможностей для защиты от опасной информации и могут открывать большие возможности для обучения базовым правилам интернет-защиты детей. В нашем буклете мы приведём полезные рекомендации по безопасному Интернету для детей.

Правила поведения в цифровой среде для детей

1. Сохранять в тайне персональные данные

Важно разъяснить ребенку недопустимость введения своих персональных данных на непроверенных и незнакомых сайтах, на которые ребенок может перейти по ссылке, указанной в рекламе, в сообщениях от незнакомых людей и т.д., распространять личную информацию в социальных сетях и мессенджерах. Регистрацию на сайтах, где необходимо вводить персональные данные, желательно проходить под присмотром родителей, так как подобного рода сайты могут быть опасны с точки зрения фейковых страниц в социальных сетях, фишинговых сайтов (использующие похожее название сайта для обмана пользователей) и др.

Какие данные не стоит размещать: дату рождения, номер телефона, адрес места жительства и обстановку квартиры, место работы родителей, информацию с банковских карт и другое.

2. Интернет — отражение реальности

Выкладывая фотографии в социальные сети, помните, что они могут стать доступными всем для просмотра. Не стоит размещать фотографии, на которых изображена семья, квартира, школа и другие личные данные. Категорически нельзя выкладывать фотографии документов!

3. Общение только со знакомыми

В мессенджерах и социальных сетях стоит общаться только с теми, с кем дети лично знакомы. Если кто-то добавляет ребенка в «друзья» в социальной сети, необходимо посоветоваться с родителями о том, безопасно ли добавлять незнакомого человека.

4. Не вся информация правдива

Информации на просторах Интернета очень много. Родителям необходимо научить ребенка избирательно относиться к полученной информации, следить на какие сообщества в социальных сетях и мессенджерах он подписан. При наличии сомнений в правдивости какой-то информации ребенку следует обратиться за советом к взрослым.

5. Уважение и соблюдение норм

Интернет, а тем более личные страницы в социальных сетях не анонимны! Важно объяснить ребенку, что нельзя делать в Интернете того, что запрещено в повседневной жизни. Необходимо уважать собеседников, быть дружелюбным. Не следует писать сообщения в оскорбительной форме. Не стоит распространять информацию, которая оскорбляет человеческое достоинство и общественную нравственность, а также выражающую явное неуважение к обществу, государству, официальным государственным символам, Конституции или органам власти. Не допускается распространение недостоверной общественно значимой информации под видом достоверных сообщений. Обращайте внимание ребенка на то, что он должен аккуратно относиться и к той информации, которую ему присылают друзья по переписке. Если ребенку прислали фотографию в личных сообщениях, это не значит, что он вправе публиковать её у себя на странице.

6. Сохранность данных — в надежных паролях

Стоит использовать для разных аккаунтов (учетных записей) разные пароли и периодически менять их (не стоит использовать в качестве пароля дату своего рождения, ФИО, номер телефона). Как правило, для того чтобы пароль был надежным, рекомендуется использовать не менее 6 символов (считается, чем больше символов, тем надежнее пароль), комбинировать цифры, буквы и символы, а также использовать заглавные и прописные буквы.

Родителям необходимо рассказать ребёнку: почему никому нельзя сообщать пароли и раскрывать личную информацию.