

«Обеспечение информационной безопасности детей дошкольного возраста»

(Общие правила для родителей дошкольников)

1. Дети этого возраста должны выходить в Интернет только под присмотром родителей (или других взрослых, например старших братьев и сестер). Если есть возможность, поставьте компьютер в общей комнате. Будьте в курсе сетевой жизни Вашего ребенка. Интересуйтесь, кто их друзья в Интернет так же, как интересуетесь реальными друзьями.

2. Независимо от возраста ребенка используйте программное обеспечение, помогающее фильтровать и контролировать информацию (см. ниже раздел «Виды технической защиты»), но не полагайтесь полностью на него. Ваше внимание к ребенку - главный метод защиты. По возможности установите на компьютер и телефон ребенка программу Контентфилтрации, которая сортирует сайты по их содержанию. Программу «родительского контроля», которая позволит ограничить функциональность устройств. Вы сами сможете выбирать программы и время действия программ, которые может использовать ребенок. Остальные программы будут недоступны.

3. Обязательно объясните вашему ребенку, что общение в Интернет – это не реальная жизнь, а своего рода игра. При этом постарайтесь направить его усилия на познание мира.

4. Объясните детям, что далеко не все, что они могут прочесть или увидеть в интернет пространстве — правда.

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

6. 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, на сайт, на котором друг упоминает номер сотового телефона Вашего ребенка или Ваш домашний адрес).

7. Ограничивайте время пребывания детей в Интернете, как и время работы за компьютером, в соответствии с рекомендациями врачей и психологов для соответствующего возраста вашего ребенка.

8. Расскажите детям о конфиденциальности. Научите их никогда не выдавать в Интернете информацию о себе и своей семье (адрес, садик, возраст, реальное ФИО, любимое место прогулки, время возвращения домой, место работы отца или матери и т. д.) Если на каком-то сайте необходимо, чтобы ребенок ввел имя, помогите ему придумать псевдоним (логин), не раскрывающий никакой личной информации.

9. Научите детей не загружать файлы, программы или музыку без вашего согласия.

10. Скажите им, что никогда не стоит встречаться с друзьями из Интернета. Ведь люди могут оказаться совсем не теми, за кого себя выдают. Запретите общение с незнакомыми людьми.

11. Дайте понять, что ОН (ребенок) не один. И если столкнется с опасностью, то Вы всегда готовы выслушать и помочь. Приучите детей сообщать вам, если что-либо или кто-либо в Сети тревожит или угрожает им. Оставайтесь спокойными и напомните детям, что они в безопасности, если рассказали вам. Поощряйте ваших детей делиться с вами их успехами и неудачами в деле освоения Интернета. Приучите их спрашивать о том, в чем они не уверены.

12. Организуйте досуг, сделайте круг интересов шире, прививайте любовь к спорту и здоровому образу жизни. Научите ценить реальную и жизнь и живое человеческое общение.

13. Научите ваших детей уважать собеседников в Интернете. Объясните, что правила морали и хорошего тона одинаковы везде.

14. Регулярно повышайте свой уровень компьютерной грамотности, чтобы обезопасить себя и своего ребенка от вредоносных «новинок» сети.

ВИДЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ:

1) Защита через DNS. DNS - это преобразователь "текста" для людей (типа yandex.ru) в "адреса-числа" (типа 81.19.70.1) и наоборот. Первый этап защиты детей от нежелательного контента будет основан на том, что есть DNS сервера, которые во время "преобразования" могут ещё и фильтровать. Другими словами, если ребёнок лезет в браузере на сайт на sex.com, то такой

адрес будет преобразован в адрес, где будет предупреждение о недопустимости или что такой сайт отсутствует в сети.

2) Защита поисковой выдачи. Данный этап оградит ребёнка от нежелательных результатов поисковой выдачи. (например, при запросе «клубничка» ребенок получит информацию о ягоде, а не «ином» содержании).

3) Защита с помощью бесплатных программ и плагинов к браузеру. Сторонние бесплатные программные решения и услуги от Internet провайдеров.

4) Различные ограничения по времени нахождения ребенка в сети и за ПК.

