**Комиссия по делам несовершеннолетних и защите их прав**

**администрации г.Коврова**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

****

**ПАМЯТКА ДЛЯ РОДИТЕЛЕЙ**

**ПО БЕЗОПАСНОМУ ИНТЕРНЕТУ**

1. **Контентные риски**

 Это содержание информации Интернета как виртуальное пространство риска: различные материалы (тексты, картинки, аудио и видеофайлы, ссылки на сторонние ресурсы). Столкнуться с ними можно практически везде: социальные сети, блоги, торренты, персональные сайты, видеохостинги и др.

 **Рекомендации:**

* Установите на компьютере специальные программные фильтры, которые могут блокировать всплывающие окна и сайты с определенной тематикой. Почти каждый интернет-браузер обладает настройками безопасности: какой контент может быть заблокирован, а какой можно загружать на компьютер. Настройки браузера устанавливаются бесплатно. На сайте каждого разработчика можно найти подобную информацию в разделе «Безопасность». Специальные программы, называемые системами родительского контроля, позволяют родителям самим решать, какое содержание в интернете могут просматривать их дети, отсекать вредные сайты, в соответствии с введенными настройками. Такие программы позволяют смотреть отчеты о том, какие сайты посещал ребенок, сколько времени пользовался интернетом, устанавливать ограничения пользования компьютером и интернетом по времени.
* Объясните детям, что далеко не все, что они могут прочесть или увидеть в интернете – правда. Необходимо проверять информацию, увиденную в интернете. Для этого существуют определенные правила проверки достоверности информации. Вот некоторые признаки надежного сайта, информации которого можно доверять: авторство сайта, контактные данные авторов, источники информации, цель создания сайта.
* Поддерживайте доверительные отношения с вашим ребенком, чтобы всегда быть в курсе – с какой информацией он сталкивается в сети. Попав случайно на какой-либо опасный, но интересный сайт, ребенок с большой вероятностью из любопытства захочет познакомиться и с другими подобными ресурсами. Важно заметить это как можно раньше и объяснить ребенку, чем именно ему грозит просмотр подобных сайтов, а также обновить настройки безопасности браузера или программного фильтра. Помните, что невозможно всегда находиться рядом с детьми и постоянно их контролировать. Доверительные отношения с детьми, открытый и доброжелательный диалог зачастую может быть гораздо конструктивнее, чем постоянные отслеживания посещаемых сайтов и блокировки всевозможного контента.
1. **Коммуникационные риски**

 Они связаны с общением и межличностными отношениями интернет-пользователей. В поисках внимания и поддержки, общаясь в сети, дети в силу коммуникационной неопытности могут добавлять в «друзья» совершенно неизвестных им в реальной жизни людей. Детский познавательный интерес к теме сексуальных отношений между мужчиной и женщиной может активно эксплуатироваться злоумышленниками в интернете. Взрослое лицо либо объединившиеся группы сверстников обладают определенными преимуществами и возможностями психологического давления на несовершеннолетних.

**Рекомендации:**

* Объясните детям, что при общении в интернете они должны быть дружелюбными с другими пользователями, не провоцировать агрессивность других. Ни в коем случае не стоит писать оскорбительные отклики и комментарии, в том числе с употреблением грубой нецензурной бранью.
* Научите детей правильно реагировать на обидные слова или действия других пользователей. Не стоит общаться с агрессором и тем более пытаться ответить ему тем же. Возможно стоит вообще покинуть данный ресурс и удалить оттуда свою личную информацию, если не получается решить проблему мирным путем. Лучший способ испортить хулигану его выходку – отвечать ему полным игнорированием.
* Наблюдайте за эмоциональным состоянием и настроениями ребенка во время его нахождения в интернете. Поддерживайте с ним доверительные отношения, чтобы он сам мог сообщить вам о поступлении угроз либо оскорблений.
* Убедитесь, что угрозы и оскорбления из сети не перешли в реальную жизнь в виде преследования. При необходимости проконсультируйтесь со специалистами правоохранительных органов либо обратитесь туда с официальным заявлением.
* Отслеживайте, кого ребенок добавляет к себе в «друзья», с кем предпочитает общаться в сети, есть ли среди его контактов взрослых лиц, как позиционирует ребенок себя в сети. Именно завышенные личные характеристики не позволяют ребенку уже в реальной встрече сказать «нет» негативному развитию контакта.
* Объясните ребенку, что при общении на ресурсах, требующих регистрации, лучше не использовать реальное имя, либо псевдоним, позволяющие идентифицировать его. Помогите ему выбрать ник, не содержащий личной информации.
* Объясните ребенку, что такое персональные данные, правила пользования как своими, так и чужими персональными данными, ответственность за нарушение этих правил, негативные последствия доступа в социальных сетях к вашей личной переписке, к вашим фотографиям и т.п.
1. **Электронные риски**

 Это вероятность столкнуться с хищением персональной информации или подвергнуться атаке вредоносных программ.

* Установите на все домашние компьютеры антивирусные программы и специальные почтовые фильтры.
* Используйте только лицензионные программы и данные, полученные из надежных источников. Чаще всего вирусами бывают заражены пиратские копии программ, особенно компьютерные игры.
* Никогда не открывайте вложения, присланные с подозрительных и неизвестных вам адресов.
* Следите за тем, чтобы ваш антивирус постоянно обновлялся, и раз в неделю проверяйте компьютер на вирусы.
* Регулярно делайте резервную копию важных данных, а также научите это делать ваших детей.
* Старайтесь периодически менять пароли (от электронной почты, от профилей в социальных сетях), но не используйте слишком простые пароли, которые можно легко взломать (даты рождения, номера телефонов и т.п).
* Расскажите ребенку, что нельзя раскрывать никакие пароли своим друзьям и знакомым. Если пароль стал кому-то известен, то его необходимо срочно поменять.
* Расскажите ребенку. что если он пользуется интернетом с помощью чужого устройства, он должен не забывать выходить из своего аккаунта в социальной сети, в почте, и на других сайтах после завершения работы. Никогда не следует сохранять на чужом компьютере свои пароли, личные файлы, историю переписки – по этой информации злоумышленники могут многое узнать о вашем ребенке.
1. **Потребительские риски**

 Это злоупотребление в интернете правами потребителя: недобросовестная либо незаконная реклама, риск приобретения товара низкого качества, различные подделки, контрафактной и фальсифицированной продукции, потери денежных средств без приобретения товара или услуги, хищения персональной информации (номера банковских счетов, паспортные данные, коды, пароли и др.) с целью кибермошенничества и др.

**Рекомендации:**

* Проинформируйте ребенка о самых распространенных методах мошенничества в сети. Совместно принимайте решения о том, стоит ли воспользоваться теми или иными услугами, предлагаемыми в интернете.
* Не отправляйте о себе слишком много информации при совершении интернет-покупок. Никогда администратор или модератор сайта не потребует полные данные вашего счета, пароли и пин-коды. Если кто-то запрашивает подобные данные, будьте бдительны – скорее всего, это мошенники.
* Ознакомьтесь на сайте с отзывами покупателей. Избегайте предоплаты. Уточните, как долго существует магазин (в поисковике лил по дате регистрации домена – сервис Whois).
* Сравните цены в разных интернет-магазинах.
* Поинтересуйтесь возможностью получения кассового чека и других документов за покупку.
1. **Риск интернет-зависимости**

 Это навязчивое желание войти в интернет, находясь в офлайн и неспособность выйти из интернета, будучи онлайн. Это и игровая зависимость от компьютерных игр. Навязчивый веб-серфинг – бесконечные путешествия по всемирной паутине, поиск информации. Пристрастие к виртуальному общению и виртуальным знакомствам, избыточность друзей в сети.

**Рекомендации:**

* Поговорите с ребенком о том, чем он занимается в интернете. Социальные сети и компьютерные игры создают иллюзию полной занятости важным делом. Выясните, поддерживается ли интерес ребенка реальными увлечениями, или же он просто старается ничего не пропустить и следит за обновлениями ради самого процесса. Выясните, насколько важно для ребенка общение в сети и не заменяет ли оно реальное общение с друзьями.
* Отследите наличие психических и физических симптомов интернет-зависимости: как подавленность, раздражительность, беспокойство, нежелание общаться, головные боли, боли в спине, расстройство сна, снижение физической активности, потеря аппетита и т.п.
* Побеседуйте с работниками образовательной организации о поведении и успеваемости ребенка, не изменились ли они в худшую сторону, изменились ил его отношения с одноклассниками. Настораживающими факторами являются замкнутость, скрытность, нежелание идти на контакт; проявляется ли желание выйти в интернет с помощью телефона во время уроков.
* Не запрещайте ребенку пользоваться интернетом, но постарайтесь установить регламент пользования.
* Ограничьте возможность доступа к интернету только своим компьютером или компьютером в общей комнате – это позволяет легче контролировать деятельность ребенка в сети.
* В случае серьезных проблем обратитесь к специалисту.
1. **Помощь ребенку, если он уже столкнулся с какой-либо интернет-угрозой**
* Установите положительный эмоциональный контакт с ребенком, постарайтесь расположить его к разговору о том, что произошло. Расскажите о своей обеспокоенности тем, что с ним происходит. Ребенок должен понимать, что вы хотите помочь ему, и что способ и рамки разбирательства будут согласованы с ним.
* Соберите наиболее полную информацию о происшествии. Зайдите на страницы сайта, где ребенок мог получить угрозы, посмотрите списки его друзей, прочтите сообщения. При необходимости скопируйте и сохраните эту информацию, на случай, если придется обращаться в правоохранительные органы.
* В случае, если вы не уверены в своей оценке того, что могло произойти и насколько это серьезно для ребенка, или ребенок недостаточно откровенен с вами и не готов идти на контакт, обратитесь к специалисту (психолог, юрист, компьютерщик) либо порекомендуйте ребенку сделать это (телефон доверия).