

## Памятка:

### «Защити свои персональные данные в Сети»





## Памятка: Защити свои персональные данные в Сети

**Персональные данные** – это любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Это та информация, которая позволяет нам узнать человека в толпе, идентифицировать и определить как конкретную личность. Идентифицирующих данных огромное множество, к ним относятся:

- фамилия, имя, отчество;
- дата и место рождения;
- место жительства;
- номер телефона;
- адрес электронной почты;
- фотография;
- возраст;
- другие.

Так, если мы кому-то скажем, свои фамилию, имя, отчество и адрес места жительства, то нас вполне можно будет опознать как конкретное лицо. Но если мы исключим из этого набора данных фамилию или адрес места жительства, то понять, о каком человеке идет речь будет невозможно.

### Помните!

- После публикации информации в Интернете ее больше невозможно будет контролировать и удалять каждую ее копию.

### Проверяйте!

- Всегда удостоверьтесь в том, что вам известно, кому предоставляется информация, и вы понимаете, в каких целях она будет использоваться.

### Думайте!

- Благоразумно ли размещать личную информацию на собственном веб-сайте, если невозможно быть уверенным в целях ее использования?

### Обращайте внимание!

- Имена учеников, их фотографии и другая личная информация из школьного журнала может публиковаться на веб-сайте школы только с согласия учеников и их родителей.



## Как защитить персональные данные в Сети:

1. Ограничьте объем информации о себе, находящейся в Интернете. Удалите лишние фотографии, видео, адреса, номера телефонов, дату рождения, сведения о родных и близких и иную личную информацию.
2. Не отправляйте видео и фотографии людям, с которыми вы познакомились в Интернете и не знаете их в реальной жизни.
3. Отправляя кому-либо свои персональные данные или конфиденциальную информацию, убедитесь в том, что адресат — действительно тот, за кого себя выдает.
4. Если в сети Интернет кто-то просит предоставить ваши персональные данные, например, место жительства или номер школы, класса иные данные, посоветуйтесь с родителями или взрослым человеком, которому вы доверяете.
5. Используйте только сложные пароли, разные для разных учетных записей и сервисов.
6. Старайтесь периодически менять пароли.
7. Заведите себе два адреса электронной почты — частный, для переписки (приватный и малоизвестный, который вы никогда не публикуете в общедоступных источниках), и публичный — для открытой деятельности (форумов, чатов и так далее).

## Дополнительные пожелания:



- Обсудите с детьми опасные последствия предоставления личной информации.
- Пользователям никогда не следует сообщать пароли никому, даже давним друзьям. Кроме того, пароль необходимо регулярно менять.
- Интернет является общественным местом. Перед публикацией любой информации или своих фотографий (а также фотографий других людей) следует помнить, что любой сможет получить доступ к этой информации. Чтобы выяснить, какая информация о вас доступна в Интернете, используйте поисковый модуль и в качестве поискового слова введите собственное имя.
- Детям должна быть предоставлена возможность поговорить с родителями об отрицательном опыте, полученном в Интернете.

## При обнаружении опубликованных в Интернете оскорбительных текстов о ребенке или его фотографий:

- Сохраните все страницы, на которых был найден этот материал, для последующих действий.
- Если по сайту или его адресу можно определить поставщика услуг, необходимо связаться с ним. Поставщик услуг может удалить текст и, вероятно, раскрыть личность автора.
- Кроме того, можно попросить собственного оператора Интернета связаться с администратором данного сайта и запросить удаление материалов.
- Если администратор сайта отказался вам помочь, прекратите пользоваться таким ресурсом и удалите оттуда свои данные.
- Если оскорбление очень серьезное и является преступлением, обратитесь в полицию.
- Злонамеренные сообщения можно сохранять для последующих действий.
- Кроме того, можно настроить параметры программы работы с электронной почтой так, чтобы сообщения от определенного отправителя поступали в отдельную папку. В этом случае ребенку не придется их читать.
- Если известен адрес электронной почты отправителя, можно отправить копию злонамеренного сообщения поставщику услуг Интернета и попросить его удалить этот адрес электронной почты.
- Если адрес электронной почты отправителя неизвестен, обратитесь за помощью к поставщику услуг Интернета.

## Ссылки:

<http://персональныеданные.дети/>



Портал персональныеданные.дети



Здесь Вы найдете различные материалы, которые были разработаны специалистами Роскомнадзора, не только для педагогов и родителей, которые хотят помочь детям понять важность конфиденциальности личной жизни при использовании цифровых технологий, но также для молодых людей, которые с легкостью и энтузиазмом используют среду Интернет.

## КАК ОБЕСПЕЧИТЬ СОБСТВЕННУЮ БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ



Общаетесь в социальных сетях Facebook, Twitter, Instagram, Вконтакте или других



**Никогда не выкладывайте в общем доступе:**



**Не стоит размещать на своей страничке:**



дату и место рождения – эти данные могут сделать доступным номер Вашей карты социального страхования



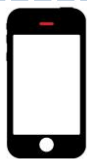
откровенные признания и фотографии – работодатели и кадровые агентства часто интересуются личными данными соискателей



планы на отпуск – можно спровоцировать ограбление



рассказы о своем рискованном поведении или хобби – страховые компании могут отказать Вам в страховке или повысить оплату за нее



домашний адрес и номер мобильного телефона – гость или собеседник могут оказаться незванными



жалобы на работодателя или коллег по работе – за резкие высказывания могут уволить



девичью фамилию Вашей мамы или название любимой песни – эти данные часто служат «ключом» при получении банковской карточки или подсказкой к паролю в аккаунте



грубости, оскорбления, матерные слова – читать такие высказывания так же неприятно, как и слышать