ИНСТРУКЦИЯ№1 для обучающихся по обеспечению информационной безопасности при использовании сети «Интернет» для размещения в учебных кабинетах, в которых осуществляется доступ в сеть «Интернет»

1. Общие положения

1. Настоящая инструкция устанавливает порядок работы обучающихся МБУ ДО»ДДТ» в сети Интернет. 2. Использование сети Интернет в Образовательном учреждении подчинено следующим принципам: - соответствия образовательным целям; - способствования гармоничному формированию и развитию личности; - уважения закона, авторских и смежных прав, а также иных прав, чести и достоинства других− граждан и пользователей Интернета; - приобретения новых навыков и знаний; - расширения применяемого спектра учебных и наглядных пособий; - социализации личности, введения в информационное общество. 3. Учащимся предоставляется доступ к работе в сети Интернет в кабинетах согласно расписанию занятий.

2. Права, обязанности и ответственность пользователей

2.1. Пользователи сети Интернет имеют право: - использовать сеть Интернет для работы с информационными ресурсами сети Интернет только в образовательных целях или для осуществления научных изысканий, выполнения гуманитарных и культурных проектов; любое нецелевое использование сети Интернет запрещено; - производить поиск необходимой информации в сети Интернет; - сохранять полученную информацию на съемном диске (дискете, CD-ROM, флешнакопителе);− съемные диски должны предварительно проверяться на наличие вирусов; получать консультации по вопросам, связанным с использованием сети Интернет. 2.2. Пользователи сети Интернет обязаны: - выполнять все требования педагога; -использовать только собственные регистрационное имя (логин) и пароль; -сохранять оборудование в целости и сохранности; -поставить в известность педагога при возникновении технических проблем. 2.3. Пользователям сети Интернет запрещается: - осуществлять действия, запрещенные законодательством РФ; -посещать сайты, содержащие информацию, запрещенную к распространению в Российской Федерации и/или не совместимую с задачами образования и воспитания в соответствии с утвержденными классификаторами; -передавать информацию, представляющую коммерческую или государственную тайну; -распространять информацию, порочащую честь и достоинство граждан; -осуществлять действия, направленные на «взлом» любых компьютеров, находящихся как в локальной сети образовательного учреждения, так и за его пределами; - использовать возможности сети Интернет для пересылки и записи непристойной, клеветнической, оскорбительной, угрожающей и порнографической продукции, материалов и информации; - работать под чужим регистрационным именем, сообщать кому-либо свой пароль, одновременно входить в систему более чем с одной рабочей станции; - устанавливать какое-либо дополнительное программное обеспечение и/или вносить какие-либо изменения в программное обеспечение, установленное как на рабочей станции, так и на сервере; производить запись информации на жесткий диск рабочей станции; работать с объемными ресурсами (video, audio, chat, игры и др.); -изменять конфигурацию компьютеров, в том числе менять системные настройки компьютера и− всех программ, установленных на нем (заставки, фоновые рисунки рабочего стола, стартовые страницы браузеров); -включать, выключать и перезагружать компьютер без согласования с педагогом. 2.4. Пользователи сети Интернет несут ответственность: - за содержание передаваемой, сознательно принимаемой и печатаемой информации; - пользователи, не соблюдающие настоящий регламент работ, лишаются права работы в сети− Интернет; -при нанесении любого ущерба (порча имущества, вывод оборудования из рабочего состояния) пользователь несет материальную ответственность.

**Инструкции№2 для обучающихся по обеспечению информационной безопасности при использовании сети «Интернет» для размещения в учебных кабинетах, в которых осуществляется доступ в сеть «Интернет»**



1. **В интернете не стоит переходить по ссылкам и нажимать кнопки во всплывающих сообщениях, которые кажутся подозрительными*.***

Не загружайте приложения, которые кажутся вам странными или находятся на неизвестном сайте. Не уверены, что письмо настоящее? Задайте себе следующие вопросы: не подозрительный ли у отправителя адрес электронной почты? Используется ли безличное приветствие? Много ли орфографических ошибок? Пытается ли автор письма создать ощущение срочности?

1. **Для защиты личной информации придумайте надежный пароль и никому его не сообщайте. Для каждого ресурса стоит использовать уникальные логины и пароли.**

Чтобы безопасно хранить разные пароли для разных учетных записей, используйте [менеджер паролей](https://infourok.ru/go.html?href=https%3A%2F%2Fwww.microsoft.com%2Fru-ru%2Fsearch%3Fq%3Dpassword%2Bmanager) и убедитесь, что для каждой учетной записи используется [сложный пароль](https://infourok.ru/go.html?href=https%3A%2F%2Fsupport.microsoft.com%2Fru-ru%2Fhelp%2F4091450%2Fwindows-protect-passwords), состоящий минимум из 10 символов — заглавных и строчных букв, чисел и специальных знаков.



1. **Никогда не предоставляйте секретные сведения, например, номер счета или пароль в ответе на сообщение электронной почты или в социальных сетях.**

Никогда не отвечайте на просьбы прислать деньги от «членов семьи», на предложения о сделке, которые слишком хороши, чтобы быть правдой, на сообщения о розыгрышах лотереи, в которых вы не участвовали, или другие мошеннические сообщения.

1. **Прежде чем вводить секретные сведения в веб-форме или на веб-странице, обратите внимание на наличие таких признаков, как адрес веб-страницы, начинающийся с префикса https и значка в виде закрытого замка рядом с адресной строкой, который обозначает безопасное соединение**

Прежде чем публиковать что-то в Интернете, спросите себя: хотите ли вы, чтобы ваши родственники и знакомые знали это? Даже такие данные, как статус ваших отношений или домашний адрес, которые могут показаться безобидными, могут быть использованы во вред, если их увидят не те люди.



1. **Для безопасности общения в социальных сетях оставляйте как можно меньше данных о себеи избирательно подходите к предложениям о дружбе.**

Не все, кого вы встречаете в Интернете, являются теми, за кого себя выдают. Киберпреступники часто создают поддельные профили в социальных сетях, чтобы вступать в переписку с доверчивыми пользователями и обирать их электронные кошельки — или делать еще что похуже.



1. **Перед просмотром входящих писем на электронном ящике, проверьте адрес отправителя. Подозрительные письма смело отправляйте в спам, особенно если в таких письмах содержатся прикрепленные файлы.**

Не открывайте подозрительные письма странного происхождения, не поддавайтесь на содержащиеся в них сомнительные предложения лёгкого заработка, не высылайте никому пароли от ваших аккаунтов, не открывайте прикреплённые к письмам подозрительные файлы и не переходите по содержащимся в них подозрительным ссылкам.

1. **Для скачивания картинки или мелодии вам предлагают отправить смс? Не спешите! Сначала проверьте этот номер в интернете — безопасен ли он и не обманут ли вас.**

Если вы все еще не уверены, свяжитесь с фигурирующей в сообщении компанией по официальным каналам, таким как веб-сайт или страница в социальных сетях. Всегда лучше проверить и перепроверить, чем рисковать своей безопасностью.