Утверждено

Директор

МОУСОШ с. Кургановка

Каменского района Пензенской области

В.В. Маркелов

Правила
работы с ресурсами сети Интернет и электронной почтой в МОУ СОШ с . Кургановка Каменского района Пензенской области

Правила использования Интернет-ресурсов на рабочем месте относятся ко всем сотрудникам (далее Пользователям) администрации, в том числе отраслевых (функциональных) органов администрации.

1. Общие положения

Глобальная сеть Интернет предоставляет доступ к ресурсам различного содержания и направленности. Использование Интернет-доступа сотрудниками разрешается и поощряется в тех случаях, когда работа с Интернет-ресурсами служит достижению целей, определенных должностными обязанностями. Интернет-доступ должен использоваться в соответствии с настоящими Правилами.

1.1. Служебные ящики электронной почты, пароли для получения доступа к Интернет, а также иным серверам или веб-страницам, не должны использоваться ни для чего иного, как для выполнения задач, непосредственно связанных со сферой деятельности.

1.2. Работа в локальной сети и/или Интернет, а также с электронной почтой будут инспектироваться и проверяться на допустимость с целью обеспечения безопасности и проверки исполнения положений, данных Правил. Также пользователи могут быть ограничены в использовании Интернет-ресурсов и/или электронной почты.

1.3. Распространение какой-либо информации через сеть Интернет, электронную почту, должно быть согласовано с вышестоящим руководителем.

1.4. Доступ к использованию служебной электронной почты сотрудникам предоставляется только для организации рабочего процесса. Почтовые сообщения, полученные или отправленные через почтовую систему не являются частной собственностью, а составляют часть внутреннего служебного документооборота.

1.5. Любые действия, произведенные на компьютере с доступом в сеть Интернет, должны соответствовать законам Российской Федерации. Нарушение этих законов влечёт за собой гражданскую или уголовную ответственность.

2. При работе с ресурсами сети Интернет запрещается:

2.1 разглашение государственной, служебной и коммерческой информации, ставшей известной сотруднику по служебной необходимости либо иным путем;
2.2. распространение защищаемых авторскими правами материалов, затрагивающих какой-либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и/или авторские и смежные с ним права третьей стороны;
2.3. публикация, загрузка и распространение материалов, содержащих вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программ для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в сети Интернет, а также размещения ссылок на вышеуказанную информацию;
2.4. не загружайте и не запускайте исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным пакетом;
2.5. не используйте анонимные прокси-серверы;
2.6. не посещайте Интернет-ресурсы, публикующие непристойные материалы, а также любые другие материалы, противоречащие общепринятым нормам морали и этики;
2.7. не создавайте и не публикуйте какие-либо замечания, предложения или материалы на Интернет-ресурсах;
2.8. не посещать Интернет-ресурсы следующего содержания в личных целях:
2.8.1. социальные сети;
2.8.2. досуг и развлечения;
2.8.3. онлайн-игры;
2.8.4. торренты;
2.8.5. казино, лотереи, тотализаторы и биржи;
2.8.6. знакомства и чаты;
2.8.7. рефераты;
2.8.8. онлайн-радио и телевидение;
2.8.9. просмотр (онлайн) или скачивание (из сети Интернет) видеофильмов.

3. Правила работы в сети Интернет

3.1. Не допускается нажимать: кнопки «Согласен», «ОК», и «Я принимаю» в баннерной рекламе, в неожиданно-всплывающих окнах или предупреждениях, на Интернет-сайтах, которые кажутся незаконными, или в предложениях удалить шпионское ПО или вирусы.
3.2. Используйте надежные антивирусные программы.
3.3. Никогда не отключайте брандмауэр.
3.4. Загружайте и скачивайте только с проверенных официальных Интернет-сайтов.
3.5. Не посещайте подозрительные Интернет-сайты. Подавляющее большинство из них содержат вирусы, непременно атакующие ваш компьютер при первом же посещении.

3.6. Используйте современные [illegible] наличии технической возможности), не дающие изменять важные файлы без ведома пользователя.
3.7. Используйте внешние носители информации только от проверенных источников.
3.8. Своевременно устанавливайте, необходимые обновления для используемого программного обеспечения.
3.9. Используйте надежные пароли (с большим количеством символов) и храните их в секрете.

4. Правила работы с электронной почтой

4.1. При работе со служебной электронной почтой запрещается:
4.1.1использовать адрес служебной электронной почты для оформления подписок, без предварительного согласования с главой города;
4.1.2.публиковать адреса других сотрудников на общедоступных Интернет-ресурсах (форумы, конференции и т. п.) без их предварительного разрешения;
4.1.3.отправлять сообщения с вложенными файлами, общий объем которых превышает 20 (двадцать) Мегабайт;
4.1.4. открывать вложенные файлы во входящих сообщениях без предварительной проверки антивирусными средствами, даже если отправитель письма хорошо известен;
4.1.5. осуществлять массовую рассылку почтовых сообщений (более 100) внешним адресатам без их на то согласия. Данные действия квалифицируются как СПАМ и являются незаконными;
4.1.6. осуществлять массовую рассылку почтовых сообщений рекламного характера без предварительного согласования с главой города;
4.1.7. рассылать через электронную почту материалы, содержащие вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в сети Интернет, а также ссылки на вышеуказанную информацию;
4.1.8. распространять защищаемые авторскими правами материалы, затрагивающие какой-либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и/или авторские и смежные с ним права третьей стороны;
4.1.9. распространять информацию, содержание и направленность которой запрещены законодательством Российской Федерации включая материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, и т. д.;
4.1.10. распространять информацию ограниченного доступа, представляющую государственную, служебную и коммерческую тайну;
4.1.11. предоставлять третьим лицам пароль доступа к своему почтовому ящику.

5. Правила работы со служебной электронной почтой.

5.1. Не допускается: открывать и загружать файлы, полученные по почте с незнакомого адреса с подозрительными расширениями.

5.2. При использовании электронной почты обращайте внимание на содержание писем. Помните, что любые заявления, сделанные в ходе электронной переписки имеют точно такой же вес, как и письменные, и могут быть использованы против Вас и/или учреждения/организации.

5.3. Доступ к почтовым веб-услугам (например, Hotmail, Mail.ru и т.д.) разрешается, но с соблюдением настоящих Правил.

6. Заключительные положения

6.1. Невыполнение условий настоящих Правил может повлечь за собой дисциплинарные взыскания предусмотренные законодательством Российской Федерации.