Регистрационный № 76

СОГЛАСОВАНО
Совет Учреждения
МАДОУ №1 «Сказка»
Протокол № 3
«20» 06 2018г.

УТВЕРЖДЕНО
приказом заведующего
МАДОУ №1 «Сказка»
_____ О.Б. Домошенко
от «25» 06 2018г.№ 123-О

Инструкция
пользователя по компьютерной безопасности при работе в сети интернет муниципальным автономным дошкольным образовательным учреждением №1«Сказка»

I. Общие положения

1.1.Инструкция пользователя по компьютерной безопасности при работе в сети Интернет муниципального автономного дошкольного образовательного учреждения №1 «Сказка» (далее по тексту – Инструкция) разработана с целью регулирования работы пользователей, распределения сетевых ресурсов коллективного пользования и содержания необходимого уровня защиты информации, ее сохранности и соблюдения прав доступа к информации, более эффективного использования сетевых ресурсов и уменьшения риска умышленного или неумышленного неправильного их использования.

1.2.Персональные компьютеры, серверы, программное обеспечение, вся информация, хранящаяся на них и вновь создаваемая, оборудование локальной вычислительной сети, коммуникационное оборудование являются собственностью муниципального автономного дошкольного образовательного учреждения №1 «Сказка» (далее по тексту – Учреждение) и представляются работникам для осуществления ими их должностных обязанностей

1.3.Персональные компьютеры, серверы, программное оборудование, оборудование ЛВС и коммуникационное, пользователи образуют систему корпоративной сети (далее по тексту – сеть)

1.4.Работа в системе каждому работнику разрешена только на определённых компьютерах, в определённое время и только с разрешёнными программами и сетевыми ресурсами. Если нужно работать вне указанного времени, на других компьютерах и с другими программами, необходимо получить разрешение руководителя.

1.5.Пользователь подключенного к сети компьютера – лицо, за которым закреплена ответственность за данный компьютер. Пользователь должен принимать все необходимые меры по защите информации и контролю за соблюдением прав доступа к ней.

1.6.Каждый сотрудник должен пользоваться только своим именем пользователя и паролем для входа в локальную сеть и сеть Интернет, передача их кому-либо запрещена.

2. Пользователи сети обязаны

2.1.Соблюдать правила работы в сети, оговорённые настоящей инструкцией.

2.2.При доступе к внешним ресурсам сети, соблюдать правила, установленные системными администраторами для используемых ресурсов.

2.3.Немедленно сообщать руководителю об обнаруженных проблемах в использовании предоставленных ресурсов, а также о фактах нарушения настоящей инструкцией кем-либо.

2.4.Не разглашать известную им конфиденциальную информацию (имена пользователей, пароли), необходимую для безопасной работы в сети.

2.5.Немедленно отключать от сети компьютер, который подозревается в заражении вирусом. Компьютер не должен подключаться к сети до тех пор, пока системные администраторы не удостоверятся в удалении вируса.

2.6.Обеспечивать беспрепятственный доступ специалистам отдела ИТО к сетевому оборудованию и компьютерам пользователей.

2.7.Выполнять предписания специалистов отдела ИТО, направленные на обеспечение безопасности сети.

2.8.В случае обнаружения неисправности компьютерного оборудования или программного обеспечения, пользователь должен обратиться к инженеру-программисту.

2.9.Не допускать посещения сайтов с потенциально вредоносным содержанием.

2.10.Быть крайне осторожным при работе с электронной почтой. Категорически запрещается открывать присоединённые к письмам, полученным от незнакомых лиц, файлы.

2.11.В обязательном порядке проверять антивирусным программным обеспечением любые внешние носители информации перед началом работы с ними.

2.12.При появлении признаков нестандартной работы компьютера («тормозит», на экране появляются и исчезают окна, сообщения, изображения, самостоятельно запускаются программы и т.п.) немедленно отключить компьютер от Ethernetсети, загрузить компьютер с внешнего загрузочного диска (CD,DVD) и провести полную антивирусную поверку всех дисков компьютера. При появлении аналогичных признаков после проделанной процедуры переустановить операционную систему с форматированием системного раздела диска.

3. Пользователи сети имеют право

3.1.Использовать в работе предоставленные им сетевые ресурсы в оговорённых в настоящей инструкции рамках. Системные администраторы вправе ограничивать доступ к некоторым сетевым ресурсам вплоть до их полной блокировки, изменять распределение трафика и проводить другие меры, направленные на повышение эффективности использования сетевых ресурсов.

3.2.Обращаться к инженеру-программисту по вопросам, связанным с распределением ресурсов компьютера. Какие-либо действия пользователя, ведущие к изменению объёма используемых им ресурсов, или влияющие на загруженность или безопасность системы (например, установка на компьютере коллективного доступа), должны санкционироваться системным администратором сети.

3.3.Обращаться за помощью к инженеру-программисту при решении задач использования ресурсов сети.

3.4.Вносить предложения по улучшению работы с ресурсом.

4. Пользователям сети Интернет запрещено

4.1.Разрешать посторонним лицам пользоваться вверенным им компьютером (кроме случаев подключения/отключения ресурсов, выполняемого инженером-программистом).

4.2.Использовать сетевые программы, не предназначенные для выполнения прямых служебных обязанностей.

4.3.Самостоятельно устанавливать или удалять установленные системным администратором сетевые программы на компьютерах, подключенных к сети Интернет, изменять настройки определённой системы и приложений, влияющие на работу сетевого оборудования и сетевых ресурсов.

4.4.Повреждать, уничтожать или фальсифицировать информацию, не принадлежащую пользователю.

4.5.Вскрывать компьютеры, сетевое и периферийное оборудование; подключать к компьютеру дополнительное оборудование без ведома системного администратора, изменять настройки BIOS, а также производить загрузку станций с дискет.

4.6.Самовольно подключать компьютер к сети, а также изменять IP-адрес компьютера, выданный системным администратором. Передача данных в сеть с использованием других IP-адресов в качестве адреса отправителя является распространением ложной информации создаёт угрозу безопасности информации на других компьютерах.

4.7.Обхождение учётной системы безопасности, системы статистики, её повреждение или дезинформация.

4.8.Использовать иные формы доступа к сети Интернет, за исключением разрешённых системным администратором: пытаться обходить установленный инженером-программистом межсетевой экран при соединении с сетью Интернет.

4.9.Осуществлять попытки несанкционированного доступа к ресурсам сети, проводить или участвовать в сетевых атаках и сетевом взломе.

4.10.Использовать сеть для совершения коммерческих сделок, распространения рекламы, коммерческих объявлений, порнографической информации, призывов к насилию, разжиганию национальной или религиозной вражды, оскорблений, угроз и т.п.

4.11.Пользователи должны уважать право других пользователей на личную информацию. Это означает, что пользователь (системный администратор) не имеет права пользоваться чужими именами и паролями для входа в сеть, читать чужую почту, причинять вред данным (кроме случаев, указанных выше), принадлежащих другим пользователям.

4.12.Запрещается производить действия, направленные на взлом (несанкционированное получение привилегированного доступа) рабочих станций и сервера Сети, равно как и любых других компьютеров в Интернет.

4.13.Закрывать доступ к информации и паролям без согласования с системным администратором.

5. Работа с электронной почтой

5.1.Электронная почта предоставляется сотрудникам Учреждения только для выполнения своих служебных обязанностей. Использование ее в личных целях запрещено.

5.2.Все электронные письма, создаваемые и хранимые на компьютерах Учреждения, являются собственностью Учреждения и не считаются персональными.

5.3.Входящие письма должны проверяться на наличие вирусов или других вредоносных программ.

5.4.Руководитель Учреждения оставляет за собой право осуществлять наблюдение за постовыми отправлениями сотрудников.

5.5.Если будет установлено, что сотрудник неправильно использует электронную почту с умыслом, ему будет вынесено дисциплинарное взыскание.

5.6.Запрещается открывать и запускать приложения, полученные по электронной почте неизвестного источника и (или) не затребованные пользователем.

5.7.Запрещается осуществлять массовую рассылку не согласованных предварительно электронных писем. Под массовой рассылкой подразумевается как рассылка множеству получателей, так и множественная рассылка одному получателю (спам).

5.8.Запрещается использовать несуществующие обратные адреса при отправке электронных писем.

6. При работе с веб-ресурсами

6.1.Пользователи используют программы для поиска информации в WWW только в случае, если необходимо для выполнения своих должностных обязанностей.

6.2.Использование ресурсы сети Интернет разрешается только в рабочих целях, использование её ресурсов не должно потенциально угрожать Учреждению.

6.3.Сотрудникам Учреждения, пользующимся Интернетом, запрещено передавать или загружать на компьютер материал, который является непристойным, порнографическим, фашистским или расистским и не относящимся к деятельности Учреждения.

6.4.Запрещено размещать в гостевых книгах, форумах, конференциях сообщения, содержащие грубые и оскорбительные выражения.

6.5.Запрещено получать и передавать через Сеть информацию, противоречащую законодательству и нормам морали общества, предоставляющую коммерческую тайну, распространять информацию, задевающую честь и достоинство граждан, а также рассылать обманные, беспокоящие и угрожающие сообщения.

6.6.Запрещено получать доступ к информационным ресурсам Сети или сети Интернет, не являющихся публичными, без разрешения их собственника.

7. Ответственность

7.1.Пользователь компьютера отвечает за информацию, хранящую на его компьютере, технически исправное состояние компьютера и вверенной техники.

7.2.Пользователь несёт личную ответственность за весь информационный обмен между его компьютером и другими компьютерами в сети и за её пределами.

7.3.За нарушение настоящей инструкции пользователь может быть отстранён от работы с Сетью.

7.4.Нарушение данной инструкции, повлекшее уничтожение, блокирование, модификацию либо копирование охраняемой законом компьютерной информации, нарушение работы компьютеров пользователей, системы или сети компьютеров, может повлечь административную или уголовную ответственность в соответствии с действующим законодательством.