Муниципальное казенное образовательное учреждение
«Ясногорская вечерняя (сменная) общеобразовательная школа»
Ясногорского района Тульской области
(МКОУ «Яв(с)ОШ»)

СОГЛАСОВАНО
Председатель первичной профсоюзной
организации МКОУ «Яв(с)ОШ»
_____ О.П.Французова
«30» августа 2013г.

УТВЕРЖДАЮ
Директор школы
_____ Н.Н.Веденеева
Приказ № 33-А
от «30» августа 2013г.

Инструкция № 23

Инструкция пользователя
по безопасной работе в сети Интернет

Персональные компьютеры, серверы, программное обеспечение, вся информация, хранящаяся на них и вновь создаваемая, коммуникационное оборудование являются собственностью МКОУ «Яв(с)ОШ» и предоставляются учащимся и учителям.

I. Общие положения:

1.1. Настоящая инструкция является дополнением к Правилам использования сети Интернет в МКОУ «Яв(с)ОШ».

1.2. Целью настоящей инструкции является регулирование работы пользователей, распределения сетевых ресурсов коллективного пользования и поддержания необходимого уровня защиты информации, ее сохранности и соблюдения прав доступа к информации.

1.3. К работе в системе допускаются лица, прошедшие инструктаж и регистрацию у ответственного за работу в сети Интернет.

1.4. Работа в системе каждому работнику разрешена только на определенных компьютерах, в определенное время и только с разрешенными программами и сетевыми ресурсами. Если нужно работать вне указанного времени, на других компьютерах и с другими программами, необходимо получить разрешение директора.

1.5. По уровню ответственности и правам доступа к СЕТИ пользователи разделяются на следующие категории: *системные администраторы* и *пользователи*.

1.6. 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.

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

1.8. Для работы на компьютере другому лицу, кроме пользователя, необходимо разрешение директора школы или работника, ответственного за Интернет.

1.9. В случае нарушения правил пользования сетью, пользователь сообщаетработнику, ответственному за Интернет, который проводит расследование причин и выявление виновников нарушений и принимает меры к пресечению подобных нарушений. Если

виновником нарушения является пользователь данного компьютера, то администрация школы имеет право отстранить виновника от пользования компьютером или принять иные меры.

1.10. Работник, следящий за правильным функционированием СЕТИ, выдает IP-адрес компьютеру, создает учетную запись электронной почты для пользователя. Самовольное подключение является серьезнейшим нарушением правил пользования СЕТЬЮ.

1.11. Работник, ответственный за Интернет информирует пользователей обо всех плановых профилактических работах, могущих привести к частичной или полной неработоспособности СЕТИ на ограниченное время, а также об изменениях предоставляемых сервисов и ограничениях, накладываемых на доступ к ресурсам СЕТИ.

1.12. Работник, ответственный за Интернет имеет право отключить компьютер пользователя от СЕТИ в случае, если с данного компьютера производились попытки несанкционированного доступа к информации на других компьютерах, и в случаях других серьезных нарушений настоящей инструкции.

1.13. Пользователь должен ознакомиться с настоящей инструкцией. Обязанность ознакомления пользователя с инструкцией лежит на работнике, ответственном за использование сети Интернет в Школе.

II. Пользователи сети Интернет обязаны:

2.1. Соблюдать правила работы в СЕТИ, оговоренные настоящей инструкцией.

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

2.3. Немедленно сообщать работнику, ответственному за использование сети Интернет об обнаруженных проблемах, а также о фактах нарушения настоящей инструкции кем-либо. Администрация школы, при необходимости, с помощью других специалистов, должна провести расследование указанных фактов и принять соответствующие меры.

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 не удален вирус.

2.6. В случае обнаружения неисправности компьютерного оборудования или программного обеспечения, пользователь должен обратиться к работнику, ответственному за функционирование техники или администрации школы.

III. Пользователи сети Интернет имеют право:

3.1. Использовать в работе предоставленные им сетевые ресурсы в оговоренных в настоящей инструкции рамках. Администрация школы 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. Какие-либо действия пользователя, ведущие к изменению объема используемых им ресурсов, или влияющие на загруженность или безопасность системы (например, установка на компьютере коллективного доступа), должны санкционироваться администрацией школы.

3.3. Обращаться за помощью к работнику, ответственному за использование сети Интернет.

3.4. Вносить предложения по улучшению работы с ресурсом.

IV. Пользователям сети Интернет запрещено:

4.1. Разрешать посторонним лицам пользоваться вверенным им компьютером.

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

4.3. Самостоятельно устанавливать или удалять установленные сетевые программы на компьютерах, подключенных к СЕТИ, изменять настройки операционной 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, изменять настройки BIOS, а также производить загрузку рабочих станций с дискет.

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

4.7. Работать с каналоемкими ресурсами (realvideo, realaudio, chat и др.)

4.8. Получать и передавать в сеть информацию, противоречащую законодательству и нормам морали общества, представляющую коммерческую или государственную тайну, распространять через сеть информацию, задевающую честь и достоинство граждан, а также рассылать обманные, беспокоящие или угрожающие сообщения.

4.9. Обхождение учетной системы безопасности, системы статистики, ее повреждение или дезинформация.

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

4.11. Использовать СЕТЬ для совершения коммерческих сделок, распространения рекламы, коммерческих объявлений, порнографической информации, призывов к насилию, разжиганию национальной или религиозной вражды, оскорблений, угроз.

4.12. Пользователи должны уважать право других пользователей на личную информацию. Это означает, что пользователь не имеет права пользоваться чужими именами и паролями для входа в сеть, читать чужую почту, причинять вред данным, принадлежащих другим пользователям.

4.13. Запрещается производить действия, направленные на взлом (несанкционированное получение привилегированного доступа) рабочих станций и сервера СЕТИ, равно как и любых других компьютеров.

4.14. Закрывать доступ к информации паролями без согласования с администрацией школы.

V. Работа с электронной почтой:

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

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

5.3. Организация оставляет за собой право получить доступ к электронной почте работников, если на то будут веские причины.

5.4. Конфигурировать программы электронной почты так, чтобы стандартные действия пользователя, использующие установки по умолчанию, были бы наиболее безопасными.

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

5.6. Почтовые сервера должны быть сконфигурированы так, чтобы отвергать письма, адресованные не на компьютеры организации.

5.7. Администрация школы организует обучение пользователей правильной работе с электронной почтой.

5.8. Справочники электронных адресов работников не могут быть доступны всем и являются конфиденциальной информацией.

5.9. Никто из посетителей не имеет права использовать электронную почту школы

5.10. Выходящие сообщения могут быть выборочно проверены, чтобы гарантировать соблюдение политики безопасности .

5.11. Пользователи не должны позволять кому-либо посылать письма от чужого имени.

5.12. Администрация школы оставляет за собой право осуществлять наблюдение за почтовыми отправлениями работников.

5.13. В качестве клиентов электронной почты могут использоваться только утвержденные почтовые программы.

5.14. Конфиденциальная информация не может быть послана с помощью электронной почты.

5.15. Если будет установлено, что работник школы с умыслом неправильно использует электронную почту , он будет наказан.

5.16. Открывать или запускать приложения, полученные по электронной почте от неизвестного источника и (или) не затребованные пользователем.

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

5.18. Использовать несуществующие обратные адреса при отправке электронных писем.

VI. При работе с веб-ресурсами:

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

6.2. Использование ресурсов сети Интернет разрешается только в рабочих целях.

6.3. По использованию сети Интернет работником школы, ответственным за Интернет ведется статистика.

6.4. Действия любого пользователя, подозреваемого в нарушении правил пользования Интернетом, могут быть запротоколированы и использоваться для принятия решения о применении к нему в санкций.

6.5. Работникам школы, пользующимся Интернетом, запрещено передавать или загружать на компьютер материал, который является непристойным, порнографическим, фашистским или расистским и не относящимся к деятельности школы.

6.6. Все файлы, загружаемые с помощью сети Интернет, должны проверяться на вирусы.

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

6.8. Запрещено получать и передавать через СЕТЬ информацию, противоречащую законодательству и нормам морали общества, распространять информацию, задевающую честь и достоинство граждан, а также рассылать обманные, беспокоящие или угрожающие сообщения.

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

VII. Ответственность:

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

7.2. Пользователь несет личную ответственность за весь информационный обмен между его компьютером и другими компьютерами в СЕТИ и за ее пределами.

7.3. За нарушение настоящей инструкции пользователь может быть отстранен 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.

Пронумеровано, прошнуровано и скреплено печатью

5 (пять) листа (ов)

Директор школы _____ Н.Н.Веденеева

М.П.