УТВЕРЖДАЮ
Директор
МАУДО г. Нижневартовска
«Детская школа искусств №1»
_____ И.В. Чижевская
«28» 08 _____ 2019 г.

РЕГЛАМЕНТ
использования информационных ресурсов сети Интернет

1. Общие положения

1.1. Настоящий регламент устанавливает единые требования по обеспечению информационной безопасности МАУДО г. Нижневартовска «Детская школа искусств №1» (далее - учреждение) при использовании ресурсов и каналов передачи данных сети Интернет.

1.2. Служебный сервис доступа к сети Интернет предназначен для обслуживания сотрудников учреждения с целью предоставления возможности оперативного получения, обработки информации, обмена информацией и повышения эффективности выполнения функциональных задач.

1.3. В настоящем Регламенте используются следующие основные термины и понятия:

браузер – специализированное ПО, являющееся средством обработки и отображения на автоматизированных рабочих местах (далее - АРМ) разных составляющих информационных систем (далее - ИС), а так же для предоставления интерфейса между ИС и её пользователем;

прокси-сервер – программный комплекс, используемый в качестве промежуточного звена между браузером и конечной ИС;

публичный сервис – ИС в сети Интернет, использование которой осуществляется на бесплатной основе или использование которой не регулируется договорными отношениями между учреждением и владельцем сервиса (его полномочным представителем).

2. Основные требования

2.1. В связи с тем, что с помощью локальной сети пользователи получают доступ к ИС учреждения, содержащим служебную информацию различной степени конфиденциальности, локальная сеть изолирована от сети Интернет. Деятельность пользователей в Интернет может контролироваться, протоколироваться и периодически проверяться ответственным за информационную безопасность работником.

2.2. На основании действующего законодательства РФ учреждение может передать информацию о действиях пользователя в сети Интернет уполномоченным на это третьим лицам, в том числе в правоохранительные органы. Использование права доступа в Интернет означает согласие пользователя с тем, что за его деятельностью осуществляется контроль.

2.3. Доступ в сеть Интернет предоставляется работникам учреждения исключительно для выполнения ими своих функциональных обязанностей. При осуществлении доступа в Интернет, в отношении информации учреждения ограниченного использования должен соблюдаться режим конфиденциальности.

2.4. Для работы в сети Интернет используются АРМ, удовлетворяющие техническим требованиям, необходимым для выполнения этих задач. В качестве программного обеспечения (далее - ПО) для в сети Интернет, рекомендуются к использованию браузеры

семейства Microsoft Internet Explorer. Возможно использование других браузеров либо лицензионных, либо свободно распространяемых, при согласовании специалистом по защите информации.

2.5. В целях контроля использования ресурсов сети Интернет, разграничения прав доступа в Интернет, снижения нагрузки на каналы передачи данных, обеспечения безопасности доступа в учреждении используется прокси-сервер. Любое ПО авторизованное для применения в учреждении и имеющее функционал доступа к ИС с использованием сети Интернет должно функционировать только через прокси-сервер.

2.6. Используемое в учреждении ПО, в том числе для доступа к ресурсам Интернет, не должно предоставлять возможности создания несанкционированных, неконтролируемых подключений из сети Интернет к локальной сети учреждения.

2.7. При работе в сети Интернет пользователям запрещается:

- использование рабочего времени и ресурсов сети Интернет в личных целях;
- посещение ресурсов, создание, распространение информационных материалов и сообщений, содержащих оскорбительную или провокационную информацию (к примеру, материалы, касающиеся сексуальных домогательств, расовых унижений, дискриминации по половому признаку, затрагивающие в оскорбительной форме вопросы возраста или сексуальной ориентации, религиозные или политические пристрастия, национальность или состояние здоровья, нарушающие законодательство РФ);
- несанкционированное распространение информации рекламного характера;
- осуществлять доступ в социальные сети в Интернет, если соответствующие функциональные обязанности не указаны в должностной инструкции;
- применять программные средства удаленного управления АРМ и использовать таковые в любом виде;
- использовать личный адрес электронной почты учреждения для регистрации в публичных сервисах, если персонализированный доступ к публичному сервису (или получение информации от публичных сервисов) не требуется для выполнения функциональных обязанностей;
- подключать к АРМ любое неавторизованное телекоммуникационное оборудование, осуществлять с помощью него доступ в Интернет на территории учреждения без согласования с директором учреждения;
- самостоятельно изменять конфигурацию ПО используемого для доступа в Интернет;
- использовать специальные программные средства обеспечения анонимности доступа в Интернет;
- подтверждать любые запросы ресурсов в сети Интернет на установку любого ПО, а так же переход на другие ресурсы Интернет, если они не известны пользователю.

2.8. Пользователи при работе в Интернет должны самостоятельно обеспечивать конфиденциальность информации учреждения, доступ к которой они получили в рамках функциональной деятельности.

2.9. Любые сообщения, кроме официальных публикаций учреждения, размещаемые пользователем в публичный доступ сети Интернет, должны включать ссылку о том, что выраженная точка зрения является личной, и не может быть расценена как официальная позиция учреждения.

2.10. Запрещенные в п. 2.7 для использования ресурсы Интернет должны блокироваться на прокси-сервере. Пользователи обязаны незамедлительно сообщать в специалисту по защите информации либо директору об обнаруженных и доступных из локальной сети незаблокированных ресурсах Интернет. Прокси-сервер протоколирует и хранит действия пользователей в сети Интернет на срок не менее чем один год. Протоколы

прокси-сервера защищаются от несанкционированного доступа.

2.11. Техническую поддержку доступа в сеть Интернет, управление соответствующими компонентами локальной сети осуществляет специалист по информационным технологиям.

2.12. Контроль выполнения требований настоящего Регламента, а также поддержание данного документа в актуальном состоянии возлагается на заместителя директора по АХР.

3. Основные правила работы

3.1. Пользователь обязан выполнять все требования специалиста по защите информации. В начале работы пользователь обязан зарегистрироваться в системе, т.е. ввести свое имя регистрации (логин) и пароль. За одним рабочим местом должно находиться не более одного пользователя. Запрещается работать под чужим регистрационным именем, сообщать кому-либо свой пароль, одновременно входить в систему более чем с одной рабочей станции.

3.2. Каждому пользователю, при наличии технической возможности, предоставляется персональный каталог, предназначенный для хранения личных файлов общим объёмом не более 100 Мб, а также возможность работы с почтовым ящиком для отправки и получения электронной почты.

3.3. Пользователю разрешается записывать полученную информацию на личные носители информации, предварительно проверенные на наличие вирусов.

3.4. Пользователю запрещено вносить какие-либо изменения в ПО, установленное как на рабочей станции, так и на серверах, а также производить без согласования со специалистом по защите информации инсталляцию ПО на жесткий диск рабочей станции.

3.5. Разрешается использовать оборудование только для работы с информационными ресурсами и электронной почтой и только в образовательных целях или для осуществления научных изысканий, выполнения гуманитарных и культурных проектов. Любое использование оборудования в коммерческих целях запрещено.

3.6. Пользователь обязан сохранять оборудование в целости и сохранности.

3.7. Пользователь обязан помнить свой пароль. В случае утраты пароля пользователь обязан сообщить системному администратору.

3.8. При нанесении любого ущерба (порча имущества, вывод оборудования из рабочего состояния) пользователь несет материальную ответственность.

3.9. При возникновении технических проблем пользователь обязан поставить в известность специалиста по информационным технологиям.