СОГЛАСОВАНО
на заседании Совета
ГБПОУ Мелеузовский
индустриальный колледж
Протокол № 2
от «16» 09 2021г.

УТВЕРЖДАЮ
Директор ГБПОУ Мелеузовский
индустриальный колледж
_____ З.Ф. Гималетдинов
«18» 09 2021 г.
Приказ № 218/1-09
от «18» 09 2021г.

Положение о работе в сети «Интернет» ГБПОУ Мелеузовский индустриальный колледж

1. Общие положения

1.1 Настоящее Положение разработано на основе Федерального закона «Об образовании в Российской Федерации» от 21.12.2012 № 273 (с изменениями и дополнениями); Федерального закона от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», Федерального закона от 7 июля 2003 года № 126-ФЗ «О связи», Федерального закона от 29.12.2010 № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" (в редакции Федерального закона от 28.07.2012 № 139-ФЗ), Федерального закона «О противодействии экстремистской деятельности» от 25.07.2002 № 114-ФЗ (с изменениями и дополнениями), а также «Методических рекомендаций по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети Интернет, причиняющей вред здоровью» (Письмо №ДЛ- 115/03 от 28 апреля 2014 года Министерства образования и науки РФ).

1.2 Для обеспечения установленных правил работы в сети Интернет в Колледже организуется функционирование системы контентной фильтрации внешнего трафика (далее СКФ), призванной ограничить доступ к нежелательным информационным ресурсам сети Интернет.

Работа в сети Интернет вне СКФ в рамках предоставляемого Колледжем доступа не допускается.

Ответственными за реализацию данного Положения в рамках своих полномочий являются лицо, ответственное за организацию и работу системы СКФ (далее — ответственный за СКФ), назначаемое приказом директора из числа работников Колледжа.

1.3 Настоящее Положение рассматривается на заседании Совета колледжа и утверждается директором Колледжа.

При разработке и обсуждении настоящего Положения Совет Колледжа руководствуется законодательством РФ и локальными нормативными документами Колледжа; опытом целесообразной и эффективной организации

учебного процесса; интересами обучающихся; целями образовательного процесса; рекомендациями профильных органов и организаций в сфере классификации ресурсов сети Интернет.

2. Основные принципы организации работы в сети интернет

2.1 Использование сети Интернет в Колледже должно быть направлено на решение задач учебно-воспитательного процесса.

Сотрудники и обучающиеся Колледжа, получившие доступ к сети Интернет в установленном порядке в рамках существующих ограничений и разрешений, имеют право:

- искать необходимую информацию;
- сохранять полученную информацию на компьютере (ноутбуке), в сети, на съемных носителях;
- распечатывать полученную информацию на принтере (при наличии технической возможности);
- передавать и размещать собственную информацию.

2.2 При работе в сети Интернет в Колледже запрещается:

- осуществлять действия, запрещенные законодательством РФ;
- посещать сайты с запрещенной в установленном порядке информацией, а также сайты с информацией, не относящейся к реализации целей образования и управления в Колледже;
- устанавливать на компьютерах (ноутбуках) без согласования с администратором ЛВС дополнительное программное обеспечение, полученное в Интернете (в том числе дополнительные браузеры, плагины, расширения);
- изменять без согласования с администратором ЛВС настройки установленного программного обеспечения для работы в сети Интернет (в том числе поисковые системы, оповещения на сайтах, домашние страницы, настройки содержимого страниц, пути сохранения загруженных файлов и проверки содержимого, настройки сетевых подключений);
- осуществлять действия, направленные на получение несанкционированного доступа к ресурсам локальной вычислительной сети Колледжа (ЛВС) по ресурсам сети Интернет.

2.3 Сотрудникам Колледжа при работе в сети Интернет запрещается размещать информацию служебного пользователя без согласования с руководством.

Информация, содержащая персональные данные сотрудника или обучающегося Колледжа, может быть размещена только с письменного согласия этого сотрудника или обучающегося (или его законного представителя).

3. Основные принципы организации системы контентной фильтрации

3.1 СКФ организуется с целью ограничения доступа пользователей сети Интернет к информации, признанной запрещенной или нежелательной.

Запрещенной признается информация, запрет на получение, размещение и распространение которой прямо установлен действующим федеральным

законодательством

Нежелательной признается информация, способная причинить вред воспитанию и здоровью обучающихся, а также информация, не направленная напрямую на реализацию целей образовательного процесса и управления в Колледже.

3.2 Ограничение доступа реализуется на основе отнесения конкретной информации к той или иной категории информации; при этом категории и относящаяся к ним информация определяются Советом Колледжа в соответствии с Перечнем видов информации, распространяемой посредством сети "Интернет", причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, направленным Письмом Министерства образования и науки РФ от 28 апреля 2014 г. № ДЛ-115/03 (далее — Перечень).

Преподаватели и другие работники Колледжа, в том числе ответственный за СКФ, могут вносить для рассмотрения Советом Колледжа предложения по отнесению конкретных ресурсов сети Интернет к той или иной категории информации.

СКФ представляет собой комплекс организационно-технических мероприятий и включает в себя:

- локальные Правила и Положения Колледжа, регулирующие функционирование СКФ,

- ограничение доступа с использованием "безопасных" публичных DNS-серверов; ограничение доступа на уровне ЛВС Колледжа;

- ограничение доступа с использованием услуг контент-фильтрации, предоставляемыхсторонними организациями;

- непосредственный контроль за работой обучающихся в сети Интернет; регулярный мониторинг состояния СКФ;

- повышение информационной компетентности в сфере кибербезопасности сотрудников, обучающихся и законных представителей.

При выборе стороннего поставщика услуг контент-фильтрации предпочтение отдается кандидатам, чьи программные и (или) аппаратные решения удовлетворят следующимтребованиям:

- масштабируемость настроек — возможность применения ограничений к отдельным пользователям, группам пользователей, ко всем пользователям;

- защита от заражений вирусами и вредоносных сайтов;

- возможность ограничения доступа по отдельные категориям в соответствии с Перечнем;

- возможность настройки нескольких различных профилей фильтрации; поддержка работы в доменах;

- совместимость с различными операционными системами (Windows XP, 7, Vista, 8, 10) и другим программным обеспечением, используемым в Колледже;

- возможность самостоятельного управления настройками фильтрации ответственным за СКФ;

- поддержка блокировки по встроенным "черным" и "белым" спискам с возможностью добавления в эти списки собственных ресурсов;

- наличие подробной статистики по фильтрации как минимум за один месяц;наличие собственной системы безопасного поиска;
- возможность использования настраиваемой страницы блокировки ресурсов;
- возможность настройки расписания работы фильтра;
- оперативная техническая поддержка по телефону;
- бесперебойная круглосуточная работа системы.

3.3 Повышение информационной компетентности в сфере кибербезопасности сотрудников, обучающихся и законных представителей может достигаться следующими способами:

3.3.1 размещение в учебных аудиториях инструкций и правил по безопасной работе в сети Интернет;

3.3.2 размещение на сайте Колледжа информации, посвященной использованию сети Интернет несовершеннолетними;

3.3.3 размещение информации о контактах, включая ссылки и телефоны, соответствующих некоммерческих организаций и органов власти, осуществляющих деятельность в сфере обеспечения информационной безопасности;

3.3.4 проведение тематических лекций, бесед, встреч силами Колледжа и (или) с привлечением сторонних специалистов;

3.3.5 сотрудничество с органами власти, образовательными и некоммерческими организациями в целях повышения информационной культуры путем осуществления совместных просветительских проектов, создания образовательных ресурсов, разработки рекомендаций и материалов.

4. Контроль за работой обучающихся в сети интернет

4.1 Пользователи локальной вычислительной сети Колледжа при работе в сети Интернет должны учитывать, что технические средства и программное обеспечение не могут обеспечить всеобъемлющую фильтрацию ресурсов сети Интернет вследствие непрерывного обновления ресурсов сети.

Для снижения вероятности обнаружения обучающимися ресурсов, попадающих под категории запрещенной или нежелательной информации, в Колледже необходимо осуществление текущего контроля при непосредственной работе студентов в сети Интернет.

4.2 Во время учебных занятий контроль работы обучающимися в сети Интернет осуществляет преподаватель, ведущий занятие.

Во время свободного доступа обучающихся к сети Интернет вне учебных занятий контроль их работы осуществляет работник Колледжа, назначаемый директором.

4.3 Преподаватель или другой работник Колледжа, осуществляющий текущий контроль:

- наблюдает за использованием компьютеров (ноутбуков) обучающимися;
- принимает меры по пресечению попыток доступа к ресурсам, не имеющим отношения к образовательному процессу;
- сообщает куратору курса о преднамеренных попытках обучающегося обратиться к ресурсам, не имеющим отношения к образовательному процессу, а также о других действиях, нарушающих установленные требования и

правила.

4.4 Колледж не несет ответственности за случайный доступ к запрещенной или нежелательной информации при соблюдении требований настоящего Положения и исправно функционирующей программно-аппаратной части СКФ.

При обнаружении наличия доступа к запрещенной или нежелательной информации обучающийся должен незамедлительно сообщить об этом преподавателю, ведущему занятие, или работнику Колледжа, осуществляющему контроль за работой студентов в сети Интернет во время свободного доступа.

Преподаватель или другой работник Колледжа при выявлении случая доступа к запрещенной или нежелательной информации должен:

- зафиксировать доменный адрес соответствующего ресурса, время и место доступа;
- прекратить использование сети Интернет обучающимися на компьютере (ноутбуке) собнаруженным доступом;
- сообщить об инциденте ответственному за СКФ с передачей зафиксированной информации;
- пресекать выявленные в дальнейшем попытки обучающихся обратиться к обнаруженному ресурсу с других компьютеров (ноутбуков) Колледжа.

Работник, ответственный за СКФ, при получении информации об обнаружении доступа к нежелательной или запрещенной информации должен самостоятельно или с помощью администратора ЛВС выявить причину инцидента и далее:

- при некорректных настройках компьютера (ноутбука) или других элементов ЛВС устранить нарушения в настройках;
- при выявленном отсутствии соответствующих ограничений нежелательной информации со стороны поставщика услуги контент-фильтрации — сообщить поставщику по каналам технической поддержки с обязательным указанием доменного адреса ресурса, времени и способе доступа;
- при выявленном отсутствии ограничения запрещенной информации — сообщить поставщику услуги контент-фильтрации, а также поставщику услуги доступа к сети Интернет (оператору связи) с обязательном указанием доменного адреса ресурса, времени и способе доступа;
- принудительно заблокировать доступ к указанному ресурсу методом "черных" списков средствами ЛВС и (или) в настройках фильтрации поставщика услуги контент- фильтрации.

4.5 При выявлении преподавателем или другим работником Колледжа необоснованного ограничения информации, относящейся к образовательному процессу, преподаватель или другой работник Колледжа должен сообщить ответственному за СКФ с указанием доменного имени ресурса, времени и месте осуществления неудачных попыток доступа.

Ответственный за СКФ при получении информации о необоснованном ограничении информации, относящейся к образовательному процессу, должен принять меры для устранения выявленных ограничений.

5. Мониторинг состояния СКФ

5.1 Мониторинг состояния СКФ (далее — Мониторинг) осуществляется ответственным за СКФ на регулярной основе.
Мониторинг включает в себя:
- отслеживание изменений федерального законодательства в сфере информационной безопасности — регулярно;
- выборочная проверка правильности настройки программно-аппаратной части СКФ на компьютерах и ноутбуках Колледжа и устранение неисправностей — не реже 1 раза в месяц;
- просмотр статистики по блокировкам, предоставляемой поставщиком услуг контентной фильтрации — еженедельно;
- реагирование на случаи некорректного предоставления или ограничения доступа в соответствии с настоящим Положением — незамедлительно при выявления подобных случаев.

По результатам Мониторинга ответственный за СКФ может выносить предложения по приведению локальных нормативных документов Колледжа в соответствие с действующим законодательством.

5.2 Выборочная проверка программно-аппаратной части СКФ должна производиться с расчетом на полный охват в течение полугода всех установленных в Колледже мест предоставления доступа к сети Интернет.

Конкретная методика выборочной проверки определяется ответственным за СКФ самостоятельно или совместно с администратором ЛВС исходя из содержания услуг контент-фильтрации, предоставляемых сторонники поставщиками, с учетом инструкций и рекомендаций поставщиков.

6. Порядок внесения изменений и пересмотра положения

Настоящее Положение пересматривается, изменяется и дополняется по мере необходимости.

Изменения и дополнения к настоящему Положению рассматриваются в составленной редакции на заседании Совета колледжа и утверждаются директором Колледжа.

После принятия новой редакции Положения предыдущее Положение утрачивает силу.