**ЧПОУ «ОБНИНСКИЙ ГУМАНИТАРНЫЙ КОЛЛЕДЖ»**

УТВЕРЖДАЮ

Директор ЧПОУ «Обнинский

Гуманитарный Колледж»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Жарвис К.С.

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_\_г.

утверждено и введено в действие

приказ № \_\_\_\_ от «\_\_\_»\_\_\_\_\_2019г.

**ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

**1. ОБЩИЕ ПОЛОЖЕНИЯ**

1.1. В соответствии с Федеральным законом от 27.07.2006 г, № 149-ФЗ (с изменениями на 06.07.2016 г.) «Об информации, информационных технологиях и о защите информации», «Доктриной информационной безопасности Российской Федерации», утвержденной Президентом Российской Федерации от 09.09.2000 г. Частное профессиональное образовательное учреждение «Обнинский Гуманитарный Колледж» (далее - Колледж) вводит отдельные правила, направленные на обеспечение безопасности и приватности данных, управляемости информационной инфраструктурой.

1.2. Политика вводится для основных информационно-технологических (ИТ) ресурсов и процессов Колледжа.

1.3. ИТ ресурсы являются неотъемлемой частью деятельности Колледжа.

1.4. Колледж предоставляет пользователям (преподавателям и обучающимся) в пользование свои ИТ ресурсы. Руководство колледжа ожидает от пользователей следования правилам, регламентам и процедурам Колледжа, локальным нормативным документам, законодательству РФ при пользовании ИТ ресурсами.

Неподчинение этим условиям влечет за собой ответственность соответствующих должностных лиц.

1.5. Директор колледжа корректирует политику ИТ безопасности, чтобы отражать изменения в законодательстве, технологиях и/или продуктах, сервисах и процессах Колледжа.

1.6. Политики объединены в настоящий документ, обязательны для ознакомления пользователями.

1.7. Контроль исполнения правил возлагается на директора Колледжа.

**2. ПРИВАТНОСТЬ И РИСКИ ПОЛЬЗОВАТЕЛЕЙ**

2.1. Колледж оставляет за собой право проводить мониторинг, копирование, запись и/или протоколирование всех действий персонала по использованию ИТ ресурсов без предупреждения. Это включает, но не ограничивается электронной почтой, ключами, логинами, паролями, доступом в Интернет и к файлам.

2.2. Пользователи не могут рассчитывать на приватность при использовании ИТ ресурсов Колледжа.

2.3. Ответственность и обязательства пользователей:

2.3.1 Эффективная информационная безопасность (ИБ) требует соответствующего участия пользователей, которые несут ответственность за свои действия и, следовательно, отвечают за все события и последствия под своим идентификационным кодом пользователя (логин/пароль).

2.3.2 Придерживаться правил и процедур доступа к сетям и системам - обязанность пользователей.

2.3.3 Ответственность пользователей включает, но не ограничивается следующим:

- считывать и передавать только данные, на которые у пользователя есть авторизованные права и которые положено знать, включая ошибочно адресованную электронную почту;

- сознательно придерживаться всех правил, законов и нормативных документов (локальных, федеральных), касающихся использованию компьютерных систем и программ;

- сообщать о нарушениях информационной безопасности ответственным за безопасность сотрудникам (директору), сотрудничать в расследованиях злоупотреблений и неправомерных действий пользователей с ИТ ресурсами;

- защищать назначенные имя и коды пользователя, пароли, другие ключи доступа от раскрытия;

- оберегать и содержать конфиденциальную печатную информацию, магнитные и электронные носители в предназначенных для этого местах, когда они не в работе и размещать их в местах, обеспечивающих их безопасность;

- использовать только приобретенное Колледжем лицензионное программное обеспечение, разрешенное для использования в Колледже, устанавливать программы и сервисы только через программиста;

- выполнять все предписания и действия по информационной безопасности (например, по антивирусной защите, пользованию электронной почтой);

- не оставлять компьютер с включенным доступом в свое отсутствие - ставить экран на пароль или выходить из системы;

**3. ПРАВИЛА ПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОЧТОЙ**

**И ДОСТУПА К РЕСУРСАМ СЕТИ ИНТЕРНЕТ**

3.1. Настоящие правила разъясняют пользователям порядок пользования ресурсами электронной почты (e-mail) и доступа к ресурсам сети Интернет.

Правила охватывают e-mail, приходящий или отправляемый через все принадлежащие Колледжу персональные компьютеры, ноутбуки, сотовые телефоны и любые другие ресурсы, способные посылать или принимать e-mail.

3.2. ИТ специалист контролирует использование e-mail, каналы доступа к ресурсам сети Интернет, чтобы гарантировать текущую доступность и надежность систем.

***3.3. Основные правила пользования электронной почтой***

3.3.1. Пользователи должны сохранять конфиденциальность своих паролей и, независимо от обстоятельств, никогда не передавать в пользование и не раскрывать их никому.

3.3.2. Пользователи должны использовать электронную почту для любой переписки, касающейся деятельности Колледжа.

3.3.3. Пользователи должны ограничивать объемы пересылаемой по e-mail информации, чтобы по возможности не перегружать и не блокировать каналы связи.

3.3.4. Пересылаемая текстовая информация при необходимости должна сжиматься стандартными архиваторами. Пересылаемая графическая информация должна сжиматься стандартными средствами пакета Office - Picture Manager (или аналог).

3.3.5. Пользователи должны готовить e-mail сообщения, соответствующие по виду и содержанию официальному статусу Колледжа.

3.3.6. Пользователи должны удалять подозрительные сообщения и сообщения от незнакомых адресатов, при этом заботиться о ежедневном обновлении антивирусной базы.

3.3.7. Приветствуется использование технологии считывания только заголовков почтовых сообщений, что резко сокращает вирусную опасность и трафик, связанный со спамом.

***3.4. Этика поведения и ответственное пользование.***

3.4.1. Колледж обеспечивает пользователей каналами доступа к сети Интернет для облегчения коммуникаций и поддержки ежедневных рабочих операций.

**Этично и приемлемо:**

- связываться и обмениваться информацией согласно с целями, характером и задачами Колледжа;

- использовать общепринятую лексику и ограничения в словесных описаниях, принятых в Колледже;

- уважать легальную защиту, которую предусматривают различные права пользования и лицензии на ПО и данные;

- придерживаться грамотного ведения e-mail, удалять устаревшие сообщения.

**Запрещено:**

- нарушать требования, правил информационной безопасности Колледжа;

- публиковать, показывать или передавать любую информацию или данные, содержащие клевету, ложь, неточности, оскорбления, непристойности, порнографию, богохульство, сексуальные домогательства, угрозы, расовые и национальные обиды и агрессивные комментарии, дискриминацию по полу, цвету волос и пр. или неверный материал;

- нарушать приватность пользователей, данных и/или использовать информацию, содержащуюся в колледже, в личных интересах или выгоды;

- заниматься рассылкой и пересылкой писем других лиц, не связанных с исполнением должностных обязанностей или учебным процессом;

- заниматься распространением недозволенной и другой рекламы и пр.;

- намеренное размножение, разработка или использование вредоносного программного обеспечения в любых формах (вирусы, черви, трояны и пр.);

- просмотр, перехват, раскрытие или помощь в просмотре, перехвате, раскрытии e-mail, не адресованной пользователю;

- использование для ведения служебных переговоров интернет-сервиса Skype;

- посещать социальные сети «Одноклассники», «В контакте», «Facebook» и аналогичные при работе на компьютерах Колледжа, если это не предусмотрено должностными обязанностями;

- просматривать, скачивать информацию развлекательного, рекламного характера, видео и музыкальные файлы, если это не предусмотрено должностными обязанностями или поручениями руководителя.

***3.5. Антивирусная политика.***

3.5.1. Настоящая политика устанавливает требования, которым должны удовлетворять все компьютеры, подключенные к сети колледжа, требования к пользователям по антивирусной защите, гарантирующие эффективное определение и защиту от деструктивного воздействия вирусов.

3.5.2. Настоящая политика применяется ко всем компьютерам сети колледжа, каталогам общего пользования, к которым относятся персональные компьютеры, ноутбуки, терминалы, любое сетевое оборудование. Источниками вирусов могут быть e-mail, Интернет-сайты со скрытыми вредоносными активными элементами, носители информации (флоппи-диски, CD-диски, flash-диски и пр.), открытые для общего доступа папки и файлы и т. д.

3.5.3. Политика.

- Защита от внешних угроз и вирусов имеет несколько уровней:

а) защита от внешних вторжений, вирусов с Интернет-сайтов;

б) антивирусный контроль файлов и почтовых вложений с помощью антивирусных программ на рабочих местах пользователей;

в) стандартные средства операционных систем.

- На всех компьютерах сети должно быть установлено антивирусное программное обеспечение, а в некоторых случаях в сочетании с персональным брэндмауэром. Антивирус контролирует жесткий диск и память компьютера на проникновение вируса, а брэндмауэр контролирует данные, попадающие и покидающие «внутренний периметр» через

- НИКОГДА не открывать вложенные (присоединенные) к e-mail файлы или макросы от неизвестных, подозрительных или недостоверных источников особенно файлов в виде архива (расширения \*.zip, \*.rar, \*.7z,\*.cab) или исполняемого файла (\*.ехе, \*.com, \*.js, \*.wbs, \*.hta, \*.bat,\*.cmd), не переходить по ссылкам, указанным в письме. Удалять эти вложения немедленно, затем удалять их «физически» из «Корзины» (папки) удаленных. В противном случае возможно заражение компьютера с шифрованием данных пользователя на локальном ПК и данных на ПК других пользователей, подключенных к локально-вычислительной сети;

- удалять и не пересылать спам, рассылки и случайные e-mail сообщения;

- использовать технологии считывания только заголовков почтовых сообщений, что резко сокращает вирусную опасность и трафик, связанный со спамом;

- никогда не скачивать файлы с неизвестных, подозрительных и «зазывающих» Интернет-сайтов;

- запретить пользователям самостоятельно скачивать, устанавливать и запускать программы без согласования с директором;

- избегать предоставления дискового пространства для чтения/записи, кроме случаев абсолютной необходимости;

- сканировать на вирусы внешние носители информации (флоппи-диски CD- диски, flash-диски и пр.);

- при возникновении угроз, выявленных персональным брэндмауэром – НЕ разрешать доступ неизвестным Вам приложениям, обращаться к директору;

- регулярно сохранять критические данные и системные настройки в безопасных местах: в локальной основной папке (Мои документы), в резервной папке в другом разделе своего диска, на сервере, на CD-R, DVDR - носителе;

- при конфликтах в сети, замедлении работы, зависании и других необычных проявлениях в работе компьютера, всегда «останавливать», «закрывать» все программы, запускать сканирующие антивирусные программы для гарантированного лечения компьютера и информировать директора.

3.5.4. Интернет- соединение.

Это программное обеспечение должно выполняться постоянно, а также настроено для регулярного исполнения по расписанию для проверки всего содержимого жесткого диска. Кроме того, антивирусные базы должны обновляться в срок (автоматически) и содержаться в актуальном состоянии. Инфицированные вирусами компьютеры должны удаляться из сети до полного уничтожения вирусов. Работы по уничтожению вирусов, настройке запуска антивирусных процедур по расписанию выполняются специалистами системного администрирования (СА).

3.5.5. Все сотрудники, допущенные к работе с информационно технологическими ресурсами колледжа, должны неукоснительно соблюдать требования инструкции по антивирусной защите, владеть навыками работы с антивирусными инструментами.

3.5.6. Антивирусное сканирование конечные пользователи выполняют самостоятельно.

3.5.7. Любая деятельность по намеренному созданию и/или распространению вредоносных программ внутри сети колледжа (вирусы, черви, трояны, почтовые бомбы и пр.) запрещена.

3.5.8. Ответственность. К сотруднику, нарушившему эту политику, применяются меры 3.дисциплинарной ответственности.

**4. ПОЛИТИКА ПОДГОТОВКИ, ОБМЕНА И ХРАНЕНИЯ**

**ДОКУМЕНТОВ И ДАННЫХ.**

4.1. Настоящая политика устанавливает требования к содержанию, копированию, порядку обмена, хранению электронных и бумажных документов, файлов и информации внутри колледжа, между управлениями и их удаленными подразделениями, предоставлении прав пользования общими данными.

4.2. Настоящая политика охватывает все подразделения колледжа, чья деятельность связана с подготовкой, копированием, хранением, обменом документами, информацией, данными с использованием информационно-технологических ресурсов.

4.3. Персонал колледжа должен придерживаться следующих требований по подготовке, копированию, хранению, обмену документами, информацией, данными, файлами:

4.3.1 Документы по виду и содержанию должны соответствовать официальному статусу колледжа, следует употреблять общепринятую деловую лексику;

4.3.2 Документы офисных, почтовых, графических и др. стандартных приложений (Word, Excel, PowerPoint, Outlook, PhotoShop и пр. или аналоги) должны создаваться и храниться в папках Мои Документы (или аналогичной)\ все папки должны иметь понятную вложенную структуру и наименования по темам;

4.3.3 Не допускается хранение файлов, информации личного характера, не относящейся к деятельности колледжа, на персональных компьютерах;

4.3.4 Документы, предназначенные для общего пользования, после создания и обработки следует хранить в общедоступной папке — на компьютере;

4.3.5 Не допускается работа с документами без извлечения из общей папки на локальный ПК пользователя;

4.3.6 Периодически, раз в неделю удалять устаревшие версии файлов с компьютера - из папок для обмена и Мои Документы,

4.3.7 Разрешено считывать, передавать, изменять только данные, на которые у пользователя есть права и которые пользователю положено знать, включая ошибочно доступные папки и электронную почту;

4.3.8 Внутриофисный обмен файлами может выполняться через общедоступную папку на компьютере; внутриофисный обмен по электронной почте через Интернет не ограничивается;

4.3.9 Оберегать и содержать электронные носители, когда они не в работе, в предназначенных для этого контейнерах, полках, стеллажах, сейфах;

4.3.10 Не держать электронные носители на столе в пределах визуальной доступности во время отсутствия на рабочем месте.

4.4. К сотруднику, нарушившему эту политику, применяются меры дисциплинарной ответственности.

**5. ПОЛИТИКА ИНФОРМАЦИОННО-ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ**

5.1. Настоящая политика устанавливает правила, уровни предоставления и получения пользователями информационно-технической поддержки своей работы.

5.2. Доступ пользователей к информационно-техническим ресурсам обеспечивается на непрерывной основе.

5.3. Директор обязуется поддерживать все технологические ресурсы в рабочем состоянии.

Поддержка требует:

а) работ по обслуживанию и развитию технологических ресурсов;

б) работ по реагированию и устранению причин этих заявок (инцидентов), т.е. работ непосредственно по поддержке. Повторяющиеся инциденты, переходят в разряд проблем и требуют выполнения внеплановых работ.

5.4. Настоящая политика охватывает и описывает все уровни поддержки пользователей, выполняемые специалистами системного администрирования.

5.5. Выделяется уровень самопомощи и три уровня поддержки:

5.5.1 Самопомощь - когда конечный пользователь самостоятельно выполняет действия по устранению проблемы, не нарушающие безопасность сети и других пользователей, такие как перезапуск приложения или компьютера, проверка подключения всех кабелей и сетевых ресурсов, антивирусное сканирование и пр.

5.5.2 Поддержка 1-го уровня - выполняется реализация работ общего профиля:

- решение оперативных проблем персонала, задач доступа и безопасности;

- первичная диагностика сложных проблем, причин неработоспособности программ;

- устранение проблемы или переадресация по сложности на следующий уровень.

5.5.3 Поддержка 2-го уровня - выполняется реализация по работе приложений и систем:

- углубленные, содержательные консультации и обучение;

- поиск решений имеющимися средствами (без вмешательства в логику приложений), помощь в выборке и восстановлении данных и документов, (раз)доработка отчетных форм;

- обслуживание контента и администрирование.

5.5.4 Поддержка 3-го уровня - выполняется реализация работ по развитию приложений, систем, инфраструктуры:

- работа с поставщиками приложений и разработчиками;

- планирование и развертывание новых приложений, реорганизация процессов и пр.

5.6. Поддержка закрепляется по уровням за техническими специалистами.

5.7. Преподаватели должны использовать Поддержку 1-го уровня только после выполнения разрешенных процедур самопомощи.

5.8. Многократное обращение за помощью по инцидентам, устраняемым самопомощью, указывает на несоответствие преподавателя занимаемой должности.

5.9. Работы по Поддержке 3-го уровня должны выполняться на проектной основе с привлечением специалистов, консультантов, подрядчиков.

5.10. Внешние консультанты и подрядчики должны иметь максимально ограниченный доступ к информационно-техническим ресурсам колледжа, но достаточный для выполнения проектов.

5.11. Для ведения проектов со стороны колледжа ответственным лицом является директор.

5.12. К сотруднику, нарушившему эту политику, применяются меры дисциплинарной ответственности.