КИРОВСКОЕ ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ
ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
«КИРОВСКИЙ МЕДИЦИНСКИЙ КОЛЛЕДЖ»

УТВЕРЖДЕНО
Приказом директора КОГПОБУ
«Кировский медицинский колледж»
от «15» января 2016 г. № 12 б/д
_____ В.В.Шубин

ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ КИРОВСКОГО ОБЛАСТНОГО ГОСУДАРСТВЕННОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАТЕЛЬНОГО БЮДЖЕТНОГО УЧРЕЖДЕНИЯ КИРОВСКИЙ МЕДИЦИНСКИЙ КОЛЛЕДЖ В ОТНОШЕНИИ ПОЛУЧЕНИЯ, ОБРАБОТКИ, ЗАЩИТЫ И ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ И УЧАЩИХСЯ

г.Киров

2016

Общие положения

Политика конфиденциальности КОГПОБУ «Кировский медицинский колледж» (далее Положение о политике конфиденциальности – положение) в отношении получения, обработки, защиты и хранения персональных данных работников разработана в соответствии со следующими нормативно-правовыми актами:

- Конституцией Российской Федерации
- Трудовым кодексом РФ
- Кодексом РФ об административных правонарушениях от 30.12.2001 № 195-ФЗ
- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»
- Указом Президента РФ от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера»
- Уставом Кировского областного государственного профессионального образовательного бюджетного учреждения «Кировский медицинский колледж» от 27.07.2016 № 783
- Положением КОГПОБУ «Кировский медицинский колледж» о порядке получения, обработки, защиты и хранения персональных данных работников и учащихся
- другими действующими нормативно-правовыми актами

Настоящим Положением определяется порядок получения, обработки, защиты, хранения, передачи и любого другого использования персональных данных работников, учащихся, а также ведения их личных дел в соответствии с трудовым законодательством Российской Федерации (для работников), а также в соответствии с Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации (для учащихся).

Цель настоящего Положения – защита персональных данных работников и учащихся КОГПОБУ «Кировский медицинский колледж» (далее Учреждение) от несанкционированного доступа и разглашения.

В настоящем Положении используются следующие основные понятия и термины:

- **персональные данные** – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;
- **защита персональных данных** – комплекс мер технического, организационного и организационно-технического, правового характера, направленных на защиту сведений, относящихся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных – работнику);
- **персональные данные работника** – информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника;
- **персональные данные учащегося** - информация, необходимая образовательному учреждению в связи с образовательным процессом и касающаяся конкретного учащегося;
- **общедоступные персональные данные работника, учащегося** – персональные данные, доступ неограниченного круга лиц, к которым предоставлен с согласия работника, учащегося или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;
- **работник** – физическое лицо, вступившее в трудовые отношения с работодателем (образовательным учреждением);
- **работодатель** – юридическое лицо (образовательное учреждение), вступившее в трудовые отношения с работником;
- **учащийся** - физическое лицо, вступившее в образовательные отношения с образовательной организацией (образовательным учреждением);

- **обработка персональных данных** – действия (операции) с персональными данными работников, учащихся, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;
- **информационная система персональных данных** – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;
- **использование персональных данных** – действия (операции) с персональными данными, совершаемые работодателем (уполномоченным им лицом) в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении работников или других лиц либо иным образом, затрагивающих права и свободы работников или других лиц;
- **конфиденциальность персональных данных** – обязательное для соблюдения работодателем или лицом, получившим доступ к персональным данным работников, требование не допускать их распространения без согласия работника или иного законного основания;
- **уничтожение персональных данных** – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Настоящее Положение является локальным нормативным актом, который утверждается руководителем Учреждения с учетом принятого решения на Совете образовательного учреждения.

Настоящее Положение вступает в силу с момента его утверждения руководителем Учреждения и действует бессрочно, до замены его новым Положением. Все изменения в Положение вносятся путём издания приказа.

Настоящее Положение о политике конфиденциальности в КОГПОБУ «Кировский медицинский колледж» не может противоречить Положению КОГПОБУ «Кировский медицинский колледж» о порядке получения, обработки, защиты и хранения персональных данных работников и учащихся, а также действующему законодательству РФ в сфере защиты персональных данных.

Защита информации о персональных данных

Сотрудники, ответственные за информатизацию в Учреждении обеспечивают следующие меры по защите хранящейся на сервере информации:

-ограничение сетевого доступа на сервер для определенных пользователей;

-организацию в отдельном сегменте сети всех компьютеров пользователей и серверов с ограниченным доступом из физической сети;

-организацию контроля технического состояния серверов и уровней защиты и восстановления информации;

-проведение регулярного копирования информации на носители;

-ведение аудита действий пользователей и своевременное обнаружение фактов несанкционированного доступа к информации;

-сервер настроен таким образом, чтобы осуществлять возможность восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней, на любой момент времени.

Работники Учреждения, имеющие доступ к персональным данным, при пользовании доступом в сеть интернет обязаны принимать максимальные меры по обеспечению безопасности:

-установить и использовать антивирусное программное обеспечение (с обновлением баз вирусов);

-по мере возможностей устанавливать обновление для операционной системы.

Политика назначения и смены паролей в Учреждении

Настоящая Политика определяет порядок обеспечения надежных средств идентификации и проверки подлинности пользователей и администраторов, хранящих и обрабатывающих конфиденциальную информацию на автоматизированных рабочих местах (далее - АРМ) и серверах.

Ответственным за обеспечение выполнения настоящей политики является Администратор безопасности конфиденциальной информации.

Установку первичного пароля производит Администратор безопасности конфиденциальной информации или Системный администратор при создании новой учётной записи. Ответственность за сохранность первичного пароля лежит на администраторе, установившим данный пароль.

При создании первичного пароля Администратор безопасности конфиденциальной информации обязан установить опцию, требующую смену пароля при первом входе в систему, а также уведомить владельца учётной записи о необходимости произвести смену пароля.

Первичный пароль не используется при сбросе забытого пароля на учётную запись, необходима установка нового пароля.

Установку основного пароля производит пользователь при первом входе в систему с новой учётной записью.

Личные пароли должны выбираться Администраторами и пользователями с учетом следующих требований:

-длина пароля не менее шести символов;

-пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ, числа, сочетания цифр и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

Пароль не должен содержать имени учетной записи пользователя или частей полного имени пользователя длиной более двух рядом стоящих знаков;

Содержать знаки трех из четырех перечисленных категорий: латинские заглавные буквы (от A до Z), латинские строчные буквы (от a до z), цифры (от 0 до 9), отличающиеся от букв и цифр знаки (например: !, $, #, %);

При смене пароля новое значение должно отличаться от предыдущего не менее, чем в 4-х позициях.

Пользователь несет персональную ответственность за сохранение в тайне основного пароля.

Пользователям запрещается:

- Записывать пароль и хранить его в легко доступных местах, в том числе на мониторе, рабочем столе или ящиках стола;
- сообщать пароль другим лицам;
- пересылать открытым текстом в электронных сообщениях;
- подбирать пароли других пользователей.

Пользователи обязаны сообщать Администратору безопасности конфиденциальной информации о всех случаях попыток противоправных действий пользователей в отношении других пользователей.

Внеплановая смена личного пароля или удаление учетной записи пользователя в случае прекращения его полномочий организации (увольнение, перевод на другую должность) должна производиться Администратором безопасности конфиденциальной информации или Системным администратором немедленно после окончания последнего сеанса работы данного пользователя с системой.

Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, перевод на другую должность) Администратора безопасности конфиденциальной информации или Системного администратора.

В случае компрометации личного пароля пользователя автоматизированной системы должны быть немедленно предприняты меры в соответствии условиями и требованиями настоящей Политики в зависимости от полномочий владельца скомпрометированного пароля.

Хранение сотрудником (исполнителем) значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе Администратора безопасности конфиденциальной информации.

При возникновении нештатных ситуаций, форс-мажорных обстоятельств, которые влекут необходимость доступа к информации пользователя, отсутствующего на рабочем месте, по решению Руководителя может быть инициирован сброс пароля данного пользователя Администратором безопасности конфиденциальной информации или Системным администратором и осуществлен доступ к необходимой информации. По факту такого доступа составляется акт, описывающий условия осуществления доступа, который подписывается Руководителем, Администратором безопасности конфиденциальной информации и сотрудником, запросившим доступ.

Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на Администратора безопасности конфиденциальной информации.

Условия использования глобальной компьютерной сети интернет и электронной почты на рабочем месте

Глобальная компьютерная сеть Интернет (далее - сеть Интернет) предоставляет доступ к ресурсам различного содержания и направленности. Системный администратор оставляет за собой право ограничивать доступ к ресурсам сети Интернет, содержание которых не имеет отношения к исполнению служебных обязанностей, а так же к ресурсам, содержание и направленность которых запрещены международным и Российским законодательством включая материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и т.д.

Условия использования глобальной компьютерной сети интернет и электронной почты на рабочем месте предназначены для сотрудников КОГПОБУ «Кировский медицинский колледж», выполнение должностных обязанностей которых связано с использованием персональных компьютеров (далее - ПК), и определяет их полномочия, обязанности и ответственность при использовании информационных ресурсов сети Интернет.

Условия использования являются обязательными для выполнения всеми сотрудниками Учреждения - пользователями сети Интернет в части, касающейся их.

Руководители структурных подразделений, пользователи и администраторы обязаны знать и выполнять нормативные правовые акты,

затрагивающие вопросы информатизации, защиты информации и информационной безопасности в части соблюдения требований и ограничений по использованию информационных ресурсов.

Доступ к сети Интернет осуществляется с рабочего ПК пользователя. Ответственность за действия на компьютере другого сотрудника несёт пользователь ПК, с которого совершено это действие.

Порядок работы в сети интернет:

Для работы в сети интернет рекомендуется использовать Браузер «Yandex», допустимо использование браузеров Mozilla Firefox, Opera и Internet Explorer.

При работе с ресурсами сети Интернет недопустимо:

-Разглашение служебной информации Учреждения, ставшей известной сотруднику по служебной необходимости либо иным путем;

-Публикация, загрузка и распространение материалов, содержащих вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в сети Интернет, а также размещения ссылок на вышеуказанную информацию,

При работе с ресурсами сети Интернет запрещается:

-Загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным пакетом;

-Допускать к работе посторонних лиц;

-Использовать программные и аппаратные средства, позволяющие получить доступ к ресурсу, запрещенному к использованию политикой Учреждения;

-Передавать служебные данные через интернет-пейджеры, социальные сети и т.д.;

-Использовать для рабочих целей облачные хранилища: Яндекс.Диск, Dropbox и т.д.;

Пользователь обязан знать и уметь пользоваться антивирусным программным обеспечением. При обнаружении вируса он должен сообщить об этом системному администратору. Пользователю запрещается производить какие-либо действия с информацией, зараженной вирусом.

Пользователь обязан информировать системного администратора о любых нарушениях, которые могут привести к несанкционированному доступу, модификации, разрушению, удалению информационных ресурсов или сбоям в работе сети.

Порядок работы с электронной почтой:

Для исполнения задач, связанных с производственной деятельностью сотрудникам Учреждения предоставляется доступ к системе электронной почты Учреждения. Использование системы электронной почты Учреждения в других целях - запрещено.

Электронная почта является собственностью Учреждения и может быть использована только в служебных целях.

Содержимое электронного почтового ящика сотрудника может быть проверено без предварительного уведомления по требованию непосредственного либо вышестоящего руководителя.

Доступ к серверу электронной почты может быть блокирован системным администратором без предварительного уведомления, при возникновении нештатной ситуации, либо в иных случаях предусмотренных организационными документами.

Ограничения доступа

Возможны следующие ограничения доступа к сети Интернет для пользователей:
-Ограничение доступа к сети Интернет с рабочего места;
-Ограничение доступа к внешней электронной почте: mail.ru, yandcx.ru и др.;
-Ограничение к развлекательным сайтам;
-Ограничение доступа к социальным сетям: одноклассники.ru, vk.com и т.д.

Способы защиты персональных данных. Уничтожение персональных данных.

Защита персональных данных работников и учащихся представляет собой регламентированный технологический, организационный и иной процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных работников и учащихся образовательного учреждения и обеспечивающий надежную безопасность информации.

Защита персональных данных работников и учащихся от неправомерного их использования или утраты обеспечивается Учреждением за счет его средств в порядке, установленном федеральным законом.

Для обеспечения внутренней защиты персональных данных работников и учащихся руководитель Учреждения предпринимает следующие меры:

- регламентирует состав работников, функциональные обязанности которых требуют соблюдения режима конфиденциальности;
- избирательно и обоснованно распределяет документы и информацию между работниками, имеющими доступ к персональным данным;
- своевременно обеспечивает работников информацией о требованиях законодательства по защите персональных данных;
- обеспечивает организацию порядка уничтожения информации;
- проводит разъяснительную работу с работниками, имеющими доступ к персональным данным, по предупреждению утраты сведений при работе с персональными данными.

Защита сведений, хранящихся в электронных базах данных, от несанкционированного доступа, искажения и уничтожения информации, а также от иных неправомерных действий, обеспечивается разграничением прав доступа с использованием учетной записи и системой паролей.

Для обеспечения внешней защиты персональных данных работников и учащихся образовательное учреждение:

- обеспечивает порядок приема, учета и контроля деятельности посетителей;
- обеспечивает охрану территории, зданий, помещений.

Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных работников либо учащихся.

В случае выявления недостоверных персональных данных работника либо учащегося или неправомерных действий с ними на период проверки Учреждение, в лице ответственных лиц обязано осуществить блокирование персональных данных работника либо учащегося с момента обращения его самого или его законного представителя либо получения запроса уполномоченного органа по защите прав субъектов.

При выявлении неправомерных действий с персональными данными работника либо учащегося, Учреждение, в лице ответственных лиц обязано устранить допущенные нарушения не более трех рабочих дней с даты такого выявления.

В случае отзыва работником либо учащимся согласия на обработку своих

персональных данных Учреждение обязано прекратить обработку персональных данных работника либо учащегося и уничтожить их в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между работником и работодателем.

Уничтожение персональных данных

Уничтожение персональных данных может быть произведено без уничтожения носителя персональных данных.
Необходимость уничтожения носителя персональных данных появляется в случае:

-физической неисправности носителя;

- списания носителя с бухгалтерского учета Учреждения.

Уничтожение персональных данных без уничтожения носителя производится в случае:

-необходимости уничтожить персональные данные по требованию субъекта;

-очистке файлов носителя типа ППЗУ после предоставления персональных данных;

-иной необходимости уничтожения персональных данных.

В случае отсутствия необходимости в уничтожении носителя уничтожение персональных данных производится незамедлительно.
Уничтожение носителей информации проводится в присутствии комиссии, назначенной приказом руководителя Учреждения (по форме, прилагаемой к Положению «Об уничтожении персональных данных» КОГПОБУ «Кировский медицинский колледж», и сопровождается составлением Акта об уничтожении носителя информации.

Ответственность за уничтожение носителей возлагается на ответственного за организацию обработки персональных данных.

Уничтожение персональных данных на бумажных носителях:

Уничтожение персональных данных с бумажного носителя без уничтожения самого носителя производится любым подходящим способом, исключающим дальнейшую обработку этих персональных данных, с сохранением возможности обработки остальных данных бумажного носителя (удаление, вымарывание). В случае согласия субъекта персональных данных допускается уничтожение его персональных данных путем закрашивания.

Уничтожение персональных данных на бумажных и машинных носителях производится в соответствии с порядком, установленным Положением «Об уничтожении персональных данных» КОГПОБУ «Кировский медицинский колледж»

Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работников и учащихся.

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, учащегося, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном ТК РФ, Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», кодексом РФ об административных правонарушениях от 30.12.2001 № 195-ФЗ и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

Лица, в обязанность которых входит ведение персональных данных работников, учащихся, подписывают Обязательство «О неразглашении персональных данных».

За неисполнение или ненадлежащее исполнение работником либо учащимся по его вине возложенных на него обязанностей по соблюдению

установленного порядка работы со сведениями конфиденциального характера несут дисциплинарную и материальную ответственность в порядке, установленном действующим законодательством РФ.

Лица, в обязанность которых входит ведение персональных данных работников, учащихся, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Заключительные положения

Учреждение обязано ознакомить работников, учащихся с настоящим Положением о политике конфиденциальности в КОГПОБУ «Кировский медицинский колледж», а также с внесенными в него изменениями и дополнениями под роспись с указанием даты ознакомления.

Сотрудники Учреждения, имеющие доступ к персональным данным и осуществляющие их сбор, обработку, уничтожение проходят инструктаж в соответствии с требованиями Положения КОГПОБУ «Кировский медицинский колледж о порядке получения, обработки, защиты и хранения персональных данных работников и учащихся, о чём ставится отметка в Журнале инструктажа сотрудников, имеющих доступ к персональным данным с росписью инструктируемого лица и датой проведённого инструктажа.

Изменения и дополнения в настоящее Положение вносятся в порядке, установленном действующим законодательством РФ для принятия локальных нормативных актов.

Положение о политике конфиденциальности в КОГПОБУ «Кировский медицинский колледж» вступает в силу с момента утверждения и действует до принятия нового.