СОГЛАСОВАНО
на Совете ГБПОУ
«Образовательный центр с.Камышла»
Протокол от 01.09.2023г
№ 50
Нурутдинов А.А.

УТВЕРЖДАЮ
Директор ГБПОУ
«Образовательный центр с.Камышла»
Харразова Р.Р.
1 сентября 2023 г.
Приказ № 48 от 1 сентября 2023 г.

Положение о защите конфиденциальной информации в ГБПОУ «Образовательный центр с.Камышла»

1. ОПРЕДЕЛЕНИЯ

1.1. **Информация** - сведения о фактах, событиях, процессах и явлениях, о состоянии объектов (их свойствах, характеристиках), используемые (необходимые) для оптимизации принимаемых решений в процессе управления данными объектами. Информация может существовать в различных формах на носителях различных типов.

1.2. **Владелец конфиденциальной информации** - физическое или юридическое лицо, правомерно владеющее конфиденциальной информацией, ограничивающее доступ к этой информации на законном основании и принимающее меры к охране ее конфиденциальности. Владельцем информации, составляющей конфиденциальную информацию, является образовательное учреждение.

1.3. **Конфиденциальность информации** - субъективно определяемая (приписываемая) характеристика (свойство) информации, указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемая способностью системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на доступ к ней.

Конфиденциальная информация – любые сведения, составляющие служебную, коммерческую, врачебную тайну, включая персональные данные сотрудников и обучающихся.

Служебная тайна – научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства (ноу-хау)), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании, и в отношении которой обладателем такой информации введен режим коммерческой тайны. Информация может быть отнесена к служебной тайне в том, случае, если она получена, разработана в процессе осуществления трудовых правоотношений и не влечет (не может повлечь) получения прибыли обладателем такой информации. Служебную тайну организации составляют любые сведения, в том числе сведения, содержащиеся в служебной переписке, телефонных переговорах, почтовых отправлениях, телеграфных и иных сообщениях, передаваемых по сетям электрической и почтовой связи, которые стали известны работнику организации в связи с исполнением им возложенных на него трудовых обязанностей. К служебной тайне не относится информация, разглашенная образовательным учреждением самостоятельно или с её согласия, а также иная информация, ограничения доступа к которой не допускаются в соответствии с законодательством РФ.

Коммерческая тайна - режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду; научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства (ноу-хау)), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны. Информация может быть отнесена к коммерческой тайне в том, случае, если она получена, разработана в процессе осуществления трудовых правоотношений, либо в результате гражданско-правовых отношений, влекущая или могущая повлечь получение прибыли обладателем такой информации.

Врачебная тайна - информация о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иные сведения, полученные при его обследовании и лечении.

Доступ к конфиденциальной информации - ознакомление определенных лиц с информацией, составляющей тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации.

Передача конфиденциальной информации - передача информации, составляющей тайну и зафиксированной на материальном носителе, ее обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности.

Предоставление информации, составляющей тайну, - передача информации, составляющей тайну и зафиксированной на материальном носителе, ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций.

Разглашение конфиденциальной информации - действие или бездействие, в результате которых информация, составляющая тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

Безопасность информации - состояние устойчивости информации к случайным или преднамеренным воздействиям, исключающее недопустимые риски ее уничтожения, искажения или раскрытия, которые приводят к материальному ущербу владельца информации.

Безопасность информации складывается из обеспечения трех ее характеристик:

- **конфиденциальность информации** заключается в том, что она доступна только тем пользователям, которым предоставлены на то соответствующие полномочия;
- **целостность информации** предполагает, что она может быть модифицирована только субъектом, имеющим для этого соответствующие полномочия. Целостность является гарантией корректности (неизменности, работоспособности) информации в любой момент времени;

- **доступность информации** означает, что имеющий соответствующие полномочия субъект может в любое время без особых проблем получить доступ к необходимой информации.

Защита информации - комплекс мероприятий, обеспечивающий предотвращение или минимизацию наносимого владельцу информации ущерба (прямого или косвенного, материального, морального или иного) посредством нежелательного воздействия на информацию, а также разглашения (утечки), искажения (модификации), утраты (снижения степени доступности) или незаконного тиражирования информации.

Для успешного осуществления своей деятельности владелец информации может быть заинтересован в обеспечении:

- своевременного доступа (за приемлемое для него время) к необходимой информации;
- конфиденциальности (сохранения в тайне) определенной части информации;
- достоверности (полноты, точности, адекватности, целостности) информации;
- защиты от навязывания ему ложной (недостоверной, искаженной) информации (то есть от дезинформации);
- защиты части информации от незаконного ее тиражирования (защиты авторских прав, прав собственника информации и т.п.);
- разграничения ответственности за нарушения законных прав (интересов) других субъектов информационных отношений и установленных правил обращения с информацией;
- возможности осуществления непрерывного контроля и управления процессами обработки и передачи информации.

Владелец информации является уязвимым, то есть потенциально подверженным нанесению ему ущерба (прямого или косвенного, материального или морального) посредством воздействия на критичную для него информацию и ее носители либо посредством неправомерного использования такой информации. Поэтому владелец информации заинтересован в обеспечении своей информационной безопасности (в различной степени в зависимости от величины ущерба, который им может быть нанесен).

Существует несколько способов нанесения владельцу информации ущерба посредством разного рода воздействий на информацию и системы ее обработки:

- нарушение конфиденциальности (раскрытие) информации;
- нарушение целостности информации (ее полное или частичное уничтожение, искажение, фальсификация, дезинформация);
- нарушение (частичное или полное) работоспособности системы;
- вывод из строя или неправомерное изменение режимов работы компонентов системы обработки информации, их модификация или подмена, приводящая к получению неверных результатов расчетов;
- несанкционированное тиражирование открытой информации (не являющейся конфиденциальной), например, программ, баз данных, разного рода документации, и т.д. в нарушение прав собственников информации, авторских прав и т.п.

2. ОБЩИЕ ПОЛОЖЕНИЯ

Данное положение объявляет политику колледжа в отношении конфиденциальной информации, устанавливает правила обращения сотрудников колледжа с конфиденциальной информацией, является обязательным для исполнения всеми сотрудникам организации, имеющими доступ к конфиденциальной информации образовательного учреждения.

Руководитель осуществляет общее управление обеспечением режима безопасности сведений, содержащих конфиденциальную информацию.

Доступ сотрудников к конфиденциальной информации колледжа, разрешается руководством в индивидуальном порядке, исходя из должностных инструкций и интересов колледжа в соответствии с назначенными правами доступа.

Лица, допущенные к конфиденциальной информации, должны быть ознакомлены с настоящим Положением, подписать индивидуальное обязательство о неразглашении информации, содержащей персональные данные (Приложение).

Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не предусмотрено законодательством РФ.

В целях защиты персональных данных работник/обучающийся (законный представитель) имеет право:

- требовать исключения или исправления неверных или неполных персональных данных.
- на свободный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные;
- определять своих представителей для защиты своих персональных данных;
- на сохранение и защиту своей личной и семейной тайны;
- право обжаловать действия образовательного учреждения, в случае нарушения законодательства о персональных данных.

Работник/обучающийся (законный представитель) обязан:

- в установленном законодательством порядке предоставлять образовательному учреждению комплекс достоверных, документированных персональных данных;
- своевременно сообщать об изменении своих персональных данных (ставить образовательное учреждение в известность об изменении фамилии, имени, отчества, даты рождения, смены паспорта, что получает отражение в информационной базе данных, а также в документах содержащих персональные данные).

3. ИНФОРМАЦИЯ, ЯВЛЯЮЩАЯСЯ КОНФИДЕНЦИАЛЬНОЙ, И ДОСТУП К НЕЙ

Информация, владельцем которой является колледж, имеет следующую классификацию:

- открытая информация (ОИ);
- конфиденциальная информация (КИ).

Открытая информация.

Открытая информация общедоступна. Она содержится в информационных и рекламных материалах колледжа, на сайте колледжа, опубликована в средствах массовой информации.

К открытой информации относятся:

- рекламные и информационные листовки, буклеты;
- стенды;
- материалы на сайте колледжа;
- публикации в СМИ;
- статьи и методические материалы.

Конфиденциальная информация включает персональные данные обучающихся – это:

- ФИО;
- пол;
- дата рождения;
- адрес регистрации;
- фотография;
- адрес фактического проживания;
- контактный телефон;
- данные паспорта или другого удостоверяющего личность документа;
- сведения о ранее полученном образовании;
- иные данные необходимые для организации учебного процесса
- сведения о состоянии здоровья и иные медицинские сведения.

В состав персональных данных сотрудника входят:

- анкетные и биографические данные;
- фотография;
- образование;
- сведения о трудовом и общем стаже;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- сведения о заработной плате сотрудника;
- сведения о социальных льготах;
- специальность,
- занимаемая должность;
- наличие судимостей;
- адрес места жительства;
- домашний телефон;
- место работы или учебы членов семьи и родственников;
- содержание трудового договора;
- состав декларируемых сведений о наличии материальных ценностей;
- содержание декларации, подаваемой в налоговую инспекцию;
- подлинники и копии приказов по личному составу;
- личные дела и трудовые книжки сотрудников;
- основания к приказам по личному составу;

- дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
- сведения о состоянии здоровья и иные медицинские сведения;
- иные необходимые данные.

4. ПОРЯДОК ОБРАЩЕНИЯ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Сведения, составляющие конфиденциальную информацию могут быть выражены в письменной, устной и иных формах. Конфиденциальная информация, ставшая известной сотруднику из письменных, устных и иных источников, охраняется равным образом.

Конфиденциальная информация, ставшая известной сотруднику из устных источников, не должна быть им разглашена. В случае разглашения данной информации сотрудник несèт ответственность в установленном законодательством порядке.

Письменные и машинные источники информации, содержащие служебную и коммерческую тайну, полежат учѐту и специальному обозначению.

В случае необходимости оперативного доведения до заинтересованных лиц сведений, составляющих тайну, Руководителем ставится резолюция на самом документе, содержащем служебную или коммерческую тайну. Такое разрешение должно содержать перечень фамилий сотрудников, обязанных ознакомиться с документами или их исполнить, срок исполнения, другие указания, подпись руководителя и дату. Руководитель может при необходимости предусмотреть ограничения в доступе конкретных сотрудников к определенным сведениям.

Не допускается разглашение сведений, составляющих врачебную тайну лицами, которым они стали известны при обучении, исполнении профессиональных, служебных и иных обязанностей, кроме случаев, установленных в настоящем Положении.

С согласия гражданина или его законного (уполномоченного) представителя допускается передача сведений, составляющих врачебную тайну, другим гражданам, в том числе должностным лицам, в интересах обследования и лечения гражданина, для проведения научных исследований, публикации в научной литературе, использования этих сведений в учебном процессе и в иных целях.

Законными представителями являются родители, усыновители или попечители обучающегося.

Полномочия законного представителя подтверждаются следующими документами:

- родители – паспорт, свидетельство о рождении ребенка;
- опекуны – паспорт (иной документ, удостоверяющий личность), решение органа опеки и попечительства, либо решение суда об установлении опеки над лицом и назначении опекуна;
- попечители - паспорт (иной документ, удостоверяющий личность), решение органа опеки и попечительства, либо решение суда об установлении попечительства над лицом и назначении попечителя.

Уполномоченными представителями являются лица, действующие на основании нотариально удостоверенной доверенности.

Полномочия представителя подтверждаются нотариально удостоверенной доверенностью.

Под обработкой персональных данных понимается сбор, систематизация,

накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение персональных данных и любое другое использование персональных данных.

В целях обеспечения прав и свобод человека и гражданина сотрудники колледжа при обработке персональных данных руководствуются Конституцией Российской Федерации, федеральными законами, Уставом колледжа, Положением об обработке персональных данных в ГАПОУ КО КБМК

5. ОХРАНА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

В целях охраны конфиденциальной информации сотрудник обязан:

1) соблюдать установленный режим охраны такой информации;

2) не разглашать конфиденциальные сведения, ставшие ему известными из письменных, устных и иных источников и не использовать эту информацию в личных целях;

3) обеспечить невозможность утраты (целостность и сохранность, соблюдение порядка хранения) документов, содержащих указанные сведения;

4) обеспечить невозможность несанкционированного доступа к документам, содержащим конфиденциальную информацию, находящимся в его ведении;

5) при увольнении представить отчет Руководителю, либо уполномоченному лицу о документах, содержащих конфиденциальные сведения, которые указанное лицо использовало при исполнении своих трудовых обязанностей, а также передать уполномоченному лицу при прекращении трудовых отношений имеющиеся в пользовании сотрудника материальные и иные носители конфиденциальной информации.

6) работать только с теми конфиденциальными сведениями и документами, к которым он получил доступ в силу своих служебных обязанностей, знать какие конкретно сведения подлежат защите, а также строго соблюдать правила пользования ими.

Сотрудники, допущенные к служебной, коммерческой тайне, обязаны незамедлительно сообщить Руководителю образовательного учреждения о пропаже документов, машинных носителей информации, содержащих конфиденциальные сведения, а также о несанкционированном доступе лиц к такой информации, или о попытке подобного доступа.

По факту разглашения конфиденциальной информации, потери документов и иного несанкционированного доступа к конфиденциальным сведениям, проводится служебное расследование, по результатам которого виновные лица привлекаются к ответственности.

При участии в работе сторонних организаций сотрудник может знакомить их представителей со сведениями, составляющими служебную или коммерческую тайну, с разрешения Руководителя. Руководитель при этом должен определить конкретные вопросы, подлежащие рассмотрению, и указать, кому и в каком объеме может быть сообщена информация, подлежащая защите.

По общему правилу доступ посторонних лиц к сведениям, составляющим врачебную тайну, не допускается, за исключением случаев, установленных действующим законодательством, а также настоящим Положением.

Защита персональных данных представляет собой технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий

достаточно надежную безопасность информации в процессе управленческой и производственной деятельности организации.

Защита персональных данных от неправомерного их использования или утраты должна быть обеспечена в порядке, установленном действующим законодательством.

Защита включает в себя следующие меры:

- ограничение и регламентация доступа сотрудников к персональным данным с установлением конкретных прав доступа;
- строгое избирательное и обоснованное распределение документов и информации между сотрудниками организации;
- рациональное и эргономичное размещение рабочих мест сотрудников организации, имеющих доступ к персональным данным, при котором исключалась бы случайная утечка защищаемой информации;
- ознакомление сотрудников организации с требованиями нормативно-методических документов по защите информации о персональных данных;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- организация порядка уничтожения информации, содержащей персональные данные сотрудников;
- регламентация обращения документов, содержащих персональные данные, на рабочих местах сотрудников организации;
- принятие в установленном порядке меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства;
- привлечение к дисциплинарной ответственности лиц, виновных в нарушении законодательства о персональных данных.

Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать Обязательство о неразглашении информации, содержащей персональные данные.

При использовании и предоставлении для научных целей персональные данные должны быть обезличены.

6. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Сотруднику, который в связи с исполнением трудовых обязанностей получил доступ к сведениям, составляющим конфиденциальную информацию, в случае умышленного или неосторожного разглашения этой информации при отсутствии в действиях такого сотрудника состава преступления, в соответствии со ст. 192 Трудового кодекса (далее ТК РФ), выносится дисциплинарное взыскание.

Каждый сотрудник колледжа, получающий для работы конфиденциальный документ (иной материальный носитель конфиденциальной информации), содержащий информацию о персональных данных, несет ответственность за сохранность носителя и конфиденциальность информации.

Сотрудник, осуществляющий сбор сведений, составляющих коммерческую тайну, незаконными способами в целях разглашения либо незаконного использования этих сведений, а также за их разглашение или незаконное использование, совершенные из корыстной или иной личной заинтересованности и причинивший крупный ущерб организации, в соответствии со ст.183 Уголовного кодекса РФ несет уголовную

ответственность.

Лица, которым в установленном законом порядке переданы сведения, составляющие врачебную тайну, с учетом причиненного гражданину ущерба несут за разглашение врачебной тайны дисциплинарную, административную или уголовную ответственность в соответствии с законодательством Российской Федерации, законодательством субъектов Российской Федерации.

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных сотрудника/обучающегося, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством.

Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения наказывается штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью, либо арестом в соответствии с УК РФ.

Неправомерность деятельности органов государственной власти и организаций по сбору и использованию персональных данных может быть установлена в судебном порядке.

Приложение № 2
к Положению об обработке персональных данных
в ГБПОУ «Образовательный центр с.Камышла»

ОБЯЗАТЕЛЬСТВО
О НЕРАЗГЛАШЕНИИ ИНФОРМАЦИИ,
СОДЕРЖАЩЕЙ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Я,_____,
(Ф.И.О. сотрудника ГБПОУ «Образовательный центр с.Камышла»)

исполняющий (ая) должностные обязанности по замещаемой должности_____
_____
_____,
(должность, наименование структурного подразделения ГБПОУ «Образовательный центр с.Камышла»)

предупрежден(а) о том, что на период исполнения должностных обязанностей в соответствии с должностным регламентом мне будет предоставлен допуск к информации, содержащей персональные данные субъектов персональных данных. Настоящим добровольно принимаю на себя обязательства:

1. Не осуществлять незаконную передачу персональных данных и не разглашать третьим лицам информацию, содержащую персональные данные, которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей.

2. В случае попытки третьих лиц незаконно получить от меня информацию, содержащую персональные данные, сообщать об этом непосредственному руководителю.

3. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты персональных данных.

4. Не разглашать и не передавать третьим лицам известную мне информацию, содержащую персональные данные, в том числе и после прекращения права на допуск к информации, содержащей персональные данные.

5. В случае расторжения со мной государственного (муниципального) контракта обязуюсь прекратить обработку персональных данных, ставших известными мне в связи с исполнением должностных обязанностей.

Я предупрежден(а) о том, что в случае нарушения данного обязательства, а также положений, предусмотренных нормами Трудового кодекса Российской Федерации, Федерального закона «О персональных данных», буду привлечен(а) к дисциплинарной и/или иной юридической ответственности в соответствии с законодательством Российской Федерации.

_____ _____
(фамилия, инициалы) (подпись)

"___"_____г.