

Утверждаю
Директор МВЕК
В.В. Новикова

« _____ » _____ 20 ____ г.

Положение о конфиденциальной информации

1. Общие положения

Для целей настоящего Положения используются следующие основные понятия:

Конфиденциальная информация – любые сведения, составляющие служебную, коммерческую тайну, включая персональные данные соискателей/сотрудников, контрагентов – физических лиц по договорам гражданско-правового характера, абитуриентов/обучающихся, их законных представителей.

Обладатель конфиденциальной информации – лицо, которое владеет информацией, составляющей конфиденциальную информацию, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим конфиденциальной информации. Обладателем информации, составляющей конфиденциальную информацию, является Колледж.

Информация – сведения (сообщения, данные) независимо от формы их представления.

Конфиденциальная информация – служебная тайна, коммерческая тайна, персональные данные соискателей/сотрудников, контрагентов – физических лиц по договорам гражданско-правового характера, абитуриентов/обучающихся, их законных представителей и иная информация охраняемая законом и настоящим Положением.

Служебная тайна – (служебная информация ограниченного распространения) – несекретная информация, касающаяся деятельности Колледжа, ограничения на распространение которой диктуются служебной необходимостью (служебная тайна), и поступающие в Колледж документы с пометкой «Для служебного пользования» (далее «ДСП»). 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 Колледжа составляют любые сведения, в том числе сведения, содержащиеся в служебной переписке, телефонных переговорах, почтовых отправлениях, телеграфных и иных сообщениях, передаваемых по сетям электронной и почтовой связи, включая мессенджеры, которые стали известны сотруднику Колледжа в связи с исполнением трудовых обязанностей. К служебной тайне не относится информация, разглашенная Колледжем самостоятельно или с его 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 выгоду; научно-техническая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства (ноу-хау, которая имеет действительную или потенциальную 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 получение прибыли обладателем такой информации.

Персональные данные – любая информация, относящаяся к соискателю, абитуриенту, их законным представителям, сотруднику, обучающемуся, исполнителям по договору гражданско-правового договора, как субъекту персональных данных, позволяющие идентифицировать его личность.

Доступ к конфиденциальной информации – ознакомление определенных лиц с информацией, составляющей конфиденциальность, 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.

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.

II Общие положения

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

2.2. Настоящее Положение утверждается Директором и является обязательным для исполнения всеми сотрудниками организации, имеющими доступ конфиденциальной информации Колледжа.

2.3. Лица, допущенные к конфиденциальной информации, должны быть ознакомлены с настоящим Положением под подпись.

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

2.5. В установленном законом порядке субъект персональных данных дает письменное согласие на обработку своих персональных данных.

2.6. В целях защиты персональных данных субъект персональных данных имеют право:

2.6.1 Требовать исключения или исправления неверных или неполных персональных данных;

2.6.2. На свободный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные;

2.6.3. Определять своих представителей для защиты своих персональных данных;

2.6.4. На сохранение и защиту своей личной и семейной тайны;

2.6.5 Право обжаловать действия Колледжа, в случае нарушения законодательства о персональных данных.

2.7. Субъекты обязаны:

2.7.1. В установленном законодательством порядке предоставлять Колледжу комплекс достоверных, документированных персональных данных;

2.7.2. Своевременно сообщать об изменении своих персональных данных (ставить Колледж в известность об изменении фамилии, имени, отчества, даты рождения смены паспорта, что получают отражение в информационной базе данных, а также в документах, содержащих персональные данные.)

III Информация, являющаяся конфиденциальной, и доступ к ней

3.1. Перечень конфиденциальной информации Колледжа определен в Приложении 1 к настоящему Положению

3.2. Каждый сотрудник, получающий доступ к конфиденциальной информации, в том числе к персональным данным, подписывает обязательство о неразглашении конфиденциальной информации, в том числе сведений о персональных данных.

3.3. Список сотрудников Колледжа, допущенных к работе с конфиденциальной информацией, определен в Приложении 2 к настоящему Положению.

3.4. В состав персональных данных обучающегося входят:

ФИО;

фамилия, имя и отчество;

гражданство;

пол;

дата, месяц, год рождения;

сведения о состоянии здоровья;

сведения об образовании (данные аттестата, диплома);

сведения о местах работы (город, название организации, должность, сроки работы);

данные об успеваемости;

адрес регистрации;

адрес проживания;

контактная информация, включая номер телефона и электронную почту;

цифровая фотография;

видеозапись проведения вступительных испытаний;

сведения о родителях (законных представителях);

данные документа, удостоверяющего личность (серия, номер, дата и орган, выдавший документ, удостоверяющий личность) и цифровая копия паспорта;

номер СНИЛС и его цифровая копия;

номер ИНН;

сведения об оплате (при условии поступления на обучение на договорной основе), включая информацию о банковских реквизитах Субъекта.

3.5. В состав персональных данных сотрудника входят:

— фамилия, имя и отчество;

— гражданство;

— пол;

— дата, месяц, год рождения;

— сведения о состоянии здоровья;

— сведения об образовании (данные аттестата, диплома);

— сведения о местах работы (город, название организации, должность, сроки работы);

— данные об успеваемости;

— адрес регистрации;

— адрес проживания;

— контактная информация, включая электронную почту;

— цифровая фотография;

— видеозапись проведения вступительных испытаний;

— сведения о родителях;

— паспортные данные (номер, дата и место выдачи) и цифровая копия паспорта;

— номер СНИЛС и его цифровая копия;

— номер ИНН;

— различного рода сведения о размерах оплаты услуг/работ; а также о размере заработной платы самого Работника, так и других сотрудников.

IV. Порядок обращения конфиденциальной информации

- 4.1. 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.
- 4.2. Конфиденциальная информация, ставшая известной сотруднику из устных источников, не должна быть им разглашена. В случае разглашения данной информации сотрудник несёт ответственность в установленном законодательством порядке.
- 4.3. Письменные и информации, конфиденциальную информацию, подлежат учёту и специальному обозначению.
- 4.4. В случае необходимости оперативного доведения до заинтересованных лиц сведений, составляющих тайну, Директором ставится резолюция на самом документе, содержащем конфиденциальную информацию. Такое разрешение должно содержать перечень фамилий сотрудников, обязанных ознакомиться с документами или их исполнить, срок исполнения, другие указания, подпись Директора и дату. Директор может при необходимости предусмотреть ограничения в доступе конкретных сотрудников к определенным сведениям.
- 4.5. Не допускается разглашение сведений, составляющих конфиденциальную информацию лицами, которым они стали известны при обучении, исполнении профессиональных, служебных и иных обязанностей, кроме случаев, установленных в настоящем Положении.
- 4.6. С согласия гражданина или его законного (уполномоченного) представителя допускается передача сведений, составляющих конфиденциальную информацию, другим гражданам, в том числе должностным лицам.
- 4.7. Законными представителями являются родители, усыновители или попечители лица.
- 4.8. 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.
- 4.9. Уполномоченными представителями являются лица, действующие на основании нотариально удостоверенной доверенности.
- 4.10. Полномочия представителя подтверждаются нотариально удостоверенной доверенностью.
- 4.11. 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.
- 4.12. В целях обеспечения прав и свобод человека и гражданина сотрудники организации при обработке персональных данных обязаны соблюдать следующие общие требования:
- 4.13. Обработка персональных данных может осуществляться исключительно в целях оказания образовательных услуг надлежащего качества и объёма, выполнения трудового договора, в иных предусмотренных законодательством случаях;
- 4.14. При определении объема и содержания обрабатываемых персональных данных сотрудники Колледжа обязаны руководствоваться Конституцией Российской Федерации и федеральными законами.
- 4.15. Использование персональных данных возможно только в соответствии с целями, определившими их получение.
- 4.16. Персональные данные не могут быть использованы в целях причинения имущественного, физического и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о

расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.

4.17. Передача персональных данных возможна только с согласия субъекта персональных данных или его законного представителя, за исключением случаев, прямо предусмотренных законодательством.

4.18. При передаче персональных данных за пределы организации, сотрудники организации не должны сообщать эти данные третьей стороне без письменного согласия субъекта персональных данных или его законного представителя, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью гражданина или в случаях, установленных федеральным законом.

4.19. Все меры конфиденциальности при сборе, обработке и хранении персональных данных распространяются как на бумажные, так и на электронные (с использованием средств автоматизации и без использования средств автоматизации) носители информации.

4.20. Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.

4.21. Хранение персональных данных должно происходить в порядке, исключающем их утрату или их неправомерное использование.

4.22. Порядок обращения с документами и другими материальными носителями информации, содержащими служебную информацию ограниченного распространения (служебная тайна) определяется Инструкцией о порядке обращения со служебной информацией ограниченного распространения в образовательном учреждении.

V. Охрана конфиденциальной информации

5.1. В целях охраны конфиденциальной информации сотрудник обязан:

5.1.1. соблюдать установленный режим охраны такой информации.

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

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

5.1.4. обеспечить невозможность несанкционированного доступа к документам, содержащим конфиденциальную информацию, находящимся в его ведении.

5.1.5. при увольнении представить письменный отчет Директору, 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 пользования сотрудника материальные и иные носители конфиденциальной информации.

5.1.6. 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.

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

5.3. 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.

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

5.8. По общему правилу доступ посторонних лиц к сведениям, составляющим конфиденциальную информацию, за исключением установленных действующим законодательством, а также настоящим Положением.

5.9. Защита персональных данных представляет собой технологический процесс, достоверности предупреждающий конфиденциальности персональных данных и, в конечном счете, обеспечивающий надежную безопасность информации в процессе управленческой и производственной деятельности организации.

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

5.11. Защита включает в себя следующие меры:

5.11.1. ограничение и регламентация доступа сотрудников к персональным данным с установлением конкретных прав доступа;

5.11.2. строгое избирательное и обоснованное распределение документов и информации между сотрудниками организации,

5.11.3. рациональное и эргономичное размещение рабочих мест сотрудников организации, имеющих доступ к персональным данным, при котором исключалась бы случайная утечка защищаемой информации;

5.11.4. ознакомление сотрудников организации с требованиями нормативно-методических документов по защите информации о персональных данных;

5.11.5. наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;

5.11.6. организация порядка уничтожения информации, содержащей персональные данные сотрудников;

5.11.7. регламентация обращения документов, содержащих персональные данные, на рабочих местах сотрудников организации;

5.11.8. принятие в установленном порядке мер по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства;

5.11.9. привлечение к дисциплинарной ответственности лиц, виновных в нарушении законодательства о персональных данных.

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

VI. Ответственность за нарушение норм, регулирующих обработку и защиту персональных работников и обучающихся, за разглашение конфиденциальной информации

6.1. Сотрудник, 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.

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

6.3. 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.

6.4. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника / обучающегося, несут дисциплинарную,

административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством.

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

6.6. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом РФ об административных нарушениях.

Перечень конфиденциальной информации Колледжа (Владелец КИ)

1. Сводный перечень сведений конфиденциального характера (далее именуется «Перечень») составлен на основании нормативных правовых актов Российской Федерации, относящих сведения к категории конфиденциальных.
2. Конфиденциальность сведений, содержащихся в работах, документах и изданиях, определяется по настоящему развернутому Перечню, составленному в соответствии с действующим законодательством.
3. Конфиденциальность документов, составленных на основании материалов, поступивших из других организаций, определяется степенью конфиденциальности сведений, содержащихся в этих материалах.

№	Информация
1	Содержание регистров бухгалтерского учета. Включая, но не ограничиваясь: реквизиты контрагентов, информация о займах, привлекаемом финансировании Владельца КИ, условия расчетов Владельца КИ, информация о выплатах в пользу сотрудников Владельца КИ, об отчислениях Владельца КИ в гос.фонды и бюджеты, страховые и благотворительные взносы Владельца КИ, компенсационные выплаты, информация о движении имущества Владельца КИ, об учете нематериальных активов, др. Информация, касающаяся имущества.
2	Любые финансовые показатели, за исключением информации, отраженной в открытой бухгалтерской и финансовой отчетности. Включая, но не ограничиваясь: доходы и расходы Владельца КИ, приток и отток денежных средств Владельца КИ, активы и пассивы Владельца КИ, размер кредиторской и дебиторской задолженности Владельца КИ, заключения аудиторов, финансовых аналитиков и отчеты оценщиков Владельца КИ.
3	Информация об организации системы защиты информации и информационных технологий: а) о применяемых программных средствах защиты информации; б) о применяемых организационных средствах защиты информации.
4	Информация об уникальных технических настройках применяемого программного обеспечения. Включая, но не ограничиваясь: настройки и параметры конкретных видов программного обеспечения, которые обладают уникальными свойствами и сопутствуют извлечению выгоды .
5	Любые аутентификационные данные для доступа к программному обеспечению и информационным системам (корпоративным информационным сервисам, аккаунтам, личным кабинетам).

6	Информация о любых выплатах работникам. Включая, но не ограничиваясь: размер заработной платы работников, схемы определения заработной платы, компенсаций, льгот и премирования работников, системы долгосрочного премирования и опционные программы руководства, размер денежных средств, выплаченных на основании листка временной нетрудоспособности.
7	Персональные данные субъектов персональных данных.
8	Исходные тексты, программный код программного обеспечения, программных разработок и иных программ для ЭВМ, которые не находятся в открытом доступе. Включая, но не ограничиваясь: исходные тексты и программный код программного обеспечения (программ для ЭВМ), разработчиком которых является Владелец КИ, и которые находятся в закрытом доступе.
9	Любые продукты, включая их составные части (результаты интеллектуальной деятельности, механики и др), которые находятся на стадии разработки. Включая, но не ограничиваясь: исходные материалы продуктов (программный код, видеоролики, изображения, тексты, методические и иные учебные материалы, результаты интеллектуальной деятельности), которые не опубликованы в открытом доступе.
10	Результаты маркетинговых и любых количественных и качественных исследований (финансово-экономических анализов, прогнозов) деятельности Владельца КИ, перспектив и приоритетных направлений ее развития. Включая, но не ограничиваясь: документы с результатами анализа рынка, эффективности продуктов, финансово-экономических прогнозов.
11	Информация о формах, содержании и условиях заключаемых всех сделок и договоров, включая сетевое взаимодействие. Включая, но не ограничиваясь: документы, содержащие описание технологических, юридических (договорных) схем реализации проектов, рисков при реализации продуктов, договоры.
12	Информация о выявленных правовых, операционных, финансовых, репутационных и иных рисках Владельца КИ. Включая, но не ограничиваясь: документы, содержащие описание выявленных рисков при реализации продуктов и процессов Владельца КИ.
13	Отчеты о проведенных образовательных исследованиях и выявленных метриках эффективности образовательной деятельности

