

― специальность;

― адрес места жительства;

― домашний телефон;

― состав семьи;

― место работы или учебы членов семьи и родственников;

― основания к приказам по личному составу;

― анкета;

― копии документов об образовании;

― сведения о состоянии здоровья;

― фотографии и иные сведения, относящиеся к персональным данным.

Указанные документы являются конфиденциальными, хотя, учитывая их массовость и единое место обработки и хранения - соответствующий гриф ограничения на них не ставится.

Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.

Собственником информационных ресурсов (персональных данных) – является субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения этими ресурсами. Это любой гражданин, к личности которого относятся соответствующие персональные данные студент, слушатель или абитуриент колледжа. Субъект персональных данных самостоятельно решает вопрос передачи колледжу своих персональных данных.

Держателем персональных данных является колледж, которому обучающийся/студент, слушатель, абитуриент добровольно передает во владение свои персональные данные. Колледж выполняет функцию владения этими данными и обладает полномочиями распоряжения ими в пределах, установленных законодательством.

Потребителями (пользователями) персональных данных являются юридические и физические лица, обращающиеся к собственнику или держателю персональных данных за получением необходимых сведений и пользующиеся ими без права передачи и разглашения.

1. **ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

Обработка персональных данных включает в себя их получение, хранение, передачу, блокирование, защиту, уничтожение.

Получение, хранение, передача или любое другое использование персональных данных студента, слушателя или абитуриента может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия в трудоустройстве, обучении, обеспечения личной безопасности, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

Все персональные данные обучающегося/студента, слушателя, абитуриента получаются у него самого. Если персональные данные возможно получить только у третьей стороны, то субъект персональных данных должен быть уведомлен об этом заранее, и от него должно быть получено письменное согласие. Колледж должен сообщить субъекту персональных данных о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа дать письменное согласие на их получение.

Не допускается получение и обработка персональных данных субъекта о его политических, религиозных и иных убеждениях и частной жизни, а также о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных законодательством РФ.

При принятии решений относительно обучающегося/студента, слушателя, абитуриента на основании его персональных данных не допускается использование данных, полученных исключительно в результате их автоматизированной обработки или электронного получения.

В соответствии со ст. 24 Конституции РФ получение и обработка данных о частной жизни субъекта персональных данных возможно только с его письменного согласия.

Пакет анкетно-биографических и характеризующих материалов (далее пакет) студента, слушателя, абитуриента формируется после издания приказа о его приеме. Пакет обязательно содержит личную карточку соответствующей формы, а также может содержать документы, содержащие персональные данные, в порядке, отражающем процесс обучения.

Все документы хранятся в папках в алфавитном порядке фамилий обучающихся/студентов.

Пакет пополняется в процессе обучения студента, слушателя, в процессе приема абитуриента в колледж.

Под блокированием персональных данных понимается временное прекращение операций по их обработке по требованию субъекта персональных данных при выявлении им недостоверности обрабатываемых сведений или неправомерных действий в отношении его данных.

При обработке персональных данных колледж в лице директора вправе определять способы обработки, документирования, хранения и защиты персональных данных на базе современных информационных технологий.

Обучающийся/студент, слушатель, абитуриент обязан:

― передавать колледжу комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом РФ, порядком приема в колледж, иными регламентирующими документами;

― своевременно сообщать колледжу об изменении своих персональных данных.

Студент, слушатель, абитуриент имеет право на:

― полную информацию о своих персональных данных и обработке этих данных;

― свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные, за исключением случаев, предусмотренных законодательством РФ;

― определение своих представителей для защиты своих персональных данных;

― доступ к относящимся к нему медицинским данным с помощью медицинского специалиста по своему выбору;

― требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований. При отказе колледжа исключить или исправить персональные данные субъект персональных данных имеет право заявить в письменной форме колледжу о своем несогласии с соответствующим обоснованием такого несогласия.

1. **ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ**

Персональные данные добровольно передаются обучающимся/студентом, слушателем, абитуриентом непосредственно держателю этих данных и потребителям внутри колледжа исключительно для обработки и использования в работе.

Внешний доступ. К числу потребителей персональных данных вне колледже относятся:

― налоговые инспекции;

― правоохранительные органы;

― органы статистики;

― страховые агентства;

― военкоматы;

― органы социального страхования;

― пенсионные фонды;

― подразделения муниципальных органов управления.

Внутренний доступ колледжа к разряду потребителей персональных данных относятся сотрудники функциональных структурных подразделений, которым эти данные необходимы для выполнения должностных обязанностей:

― директор;

― заместители директора;

― начальник и сотрудники отдела кадров;

― сотрудники бухгалтерии;

― классные руководители;

― заведующие отделением;

― секретари;

― руководители структурных подразделений.

Личные дела обучающихся/студентов колледжа хранятся в специально отведенном месте. Для этого используются специально оборудованные шкафы, которые запираются. Личные дела располагаются в алфавитном порядке.

1. **ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ**

При передаче персональных данных обучающегося/студента, слушателя и абитуриента, работодатель должен соблюдать следующие требования:

Передача внешнему потребителю:

― передача персональных данных от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных;

― при передаче персональных данных субъекта персональных данных потребителям за пределы колледжа эти данные не должны сообщаться третьей стороне без письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта или в случаях, установленных федеральным законом;

― ответы на правомерные письменные запросы даются с разрешения директора и только в письменной форме и в том объеме, который позволяет не разглашать излишний объем персональных сведений;

― не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу;

― по возможности персональные данные обезличиваются.

Передача внутреннему потребителю. Колледж вправе разрешать доступ к персональным данным своих студентов.

1. **ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ**

Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

Защита персональных данных представляет собой жестко регламентированный 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 предприятия.

6.1. **ВНУТРЕННЯЯ ЗАЩИТА**

Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документами и базами данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий руководителями и специалистами колледжа. Для защиты персональных данных необходимо соблюдать ряд мер:

― ограничение и регламентация состава сотрудников, функциональные обязанности которых требуют конфиденциальных знаний;

― строгое избирательное и обоснованное распределение документов и информации между сотрудниками;

― рациональное размещение рабочих мест сотрудников, при котором исключалось бы бесконтрольное использование защищаемой информации;

― знание сотрудниками требований нормативно – методических документов по защите информации и сохранении тайны;

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

― определение и регламентация состава сотрудников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;

― организация порядка уничтожения информации;

― своевременное выявление нарушения требований разрешительной системы доступа сотрудниками подразделения;

― воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;

― не допускается выдача личных дел сотрудников на рабочие места. Личные дела могут выдаваться на рабочие места только директору, и в исключительных случаях, по письменному разрешению директора, руководителю структурного подразделения;

― персональные компьютеры, в которых содержатся персональные данные, должны быть защищены паролями доступа.

6.2. **ВНЕШНЯЯ ЗАЩИТА**

Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лиц, пытающихся совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и другое.

Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности предприятия, посетители, сотрудники других организационных структур.

Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе кадров.

Для защиты персональных данных обучающихся/студентов и абитуриентов необходимо соблюдать ряд мер:

― порядок приема, учета и контроля деятельности посетителей;

― порядок охраны территории, зданий, помещений, транспортных средств;

― специальные меры по защите электронных баз данных.

7.**ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, СВЯЗАННОЙ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ**

Персональная ответственность – одно из главных требований к организации функционирования системы защиты персональной информации и является обязательным условием обеспечения эффективности этой системы.

Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

Каждый сотрудник предприятия, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о персональных данных влечет дисциплинарную, административную, гражданско–правовую или уголовную ответственность граждан и юридических лиц.

*Настоящее Положение рассмотрено и принято на заседании педагогического совета ГАПОУ НСО* *«Новосибирский колледж парикмахерского искусства*», *протокол № 1 от* «29» августа 2014 г.