

УТВЕРЖДАЮ
Директор ГАПОУ СМПК
А.Н.Усевич
« 05 » 05 2023 г.



ПОЛОЖЕНИЕ

**о порядке обработки и защиты персональных данных работников
государственного автономного профессионального образовательного
учреждения**

Стерлитамакский многопрофильный профессиональный колледж

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение о порядке обработки и защиты персональных данных работников (далее – Положение) является основным локальным нормативным актом, регулирующим отношения, связанные с обработкой, получением (сбором), систематизацией (комбинированием), хранением и передачей персональных данных в ГАПОУ СМПК (далее – Колледж) с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным.

1.2. Упорядочение обращения с персональными данными имеет целью обеспечить соблюдение законных прав и интересов Колледжа и его работников в связи с необходимостью получения (сбора), записи, систематизации (комбинирования), накопления, хранения, уточнения (обновления, изменения), извлечения, использования, обезличивания, блокирования, удаления, уничтожения и передачи сведений, составляющих персональные данные.

1.3. Обработка персональных данных осуществляется с соблюдением Конституции Российской Федерации, Трудового кодекса Российской Федерации принципов и правил, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», и другими действующими нормативными правовыми актами Российской Федерации.

1.4. Сведения о персональных данных работников относятся к числу конфиденциальных (составляющих охраняемую законом тайну Колледжа). Режим конфиденциальности в отношении персональных данных снимается:

- в случае их обезличивания, блокирования, удаления, уничтожения;
- по истечении 75 лет срока их хранения;
- в других случаях, предусмотренных федеральными законами.

1.5. Настоящее Положение и изменения к нему утверждаются приказом директором Колледжа. Все работники колледжа должны быть ознакомлены под роспись с данным Положением.

2. ОСНОВНЫЕ ПОНЯТИЯ.

СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ

2.1. Для целей настоящего Положения используются следующие основные понятия:

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных); персональные данные, разрешенные субъектом персональных данных для распространения, - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Обезличивание персональных данных - действия, в результате которых

становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Конфиденциальность персональных данных — Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

2.2. В состав персональных данных работника входят:

- анкетные и биографические данные (фамилия, имя, отчество (в т.ч. прежние); год, месяц, дата и место рождения, а также иные данные, содержащиеся в удостоверении личности работника);
- образование (данные об образовании работника, наличии специальных знаний или подготовки);
- сведения о трудовом и общем стаже;
- сведения о составе семьи;
- паспортные данные;
- сведения о заработной плате сотрудника;
- сведения о социальных льготах;
- данные о профессии, специальности работника;
- занимаемая должность;
- адрес места жительства;
- мобильный (домашний) телефон;
- состав семьи;
- сведения о доходах работника;
- данные, содержащиеся в трудовой книжке и (или) сведениях о трудовой деятельности работника;
- данные, содержащиеся в документе, подтверждающем регистрацию в системе индивидуального (персонифицированного) учета, в том числе в

форме электронного документа;

- данные, содержащиеся в документе идентификационный номер налогоплательщика (ИНН) — цифровой код, упорядочивающий учёт налогоплательщиков в Российской Федерации;
- данные, содержащиеся в документах воинского учета (при их наличии);
- документы о состоянии здоровья работника;
- наличие судимостей;
- иные персональные данные, при определении объема и содержания которых работодатель руководствуется настоящим Положением и законодательством РФ.

2.3. Бумажные носители персональных данных:

- трудовая книжка;
- личные дела работников;
- журналы учета трудовых книжек;
- журнал учета командировок;
- листки нетрудоспособности;
- табели учета рабочего времени;
- личная карточка Т 2;
- входящая и исходящая корреспонденция военкомата, ОВИР, страховой компании, службы судебных приставов;
- приказы по личному составу работников;
- приказы о командировках сотрудников;
- трудовой договор;
- дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
- анкеты, заполняемые работниками;
- журналы регистрации документов;
- журналы регистрации выданных справок;
- лицевые счета, налоговые карточки, другие бухгалтерские документы, содержащие данные о доходах сотрудников;
- медицинские книжки.

3. ПОРЯДОК ПОЛУЧЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ.

3.1. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных

должно быть конкретным, предметным, информированным, сознательным и однозначным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются оператором.

Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство наличия оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью.

Порядок получения в форме электронного документа согласия субъекта персональных данных на обработку его персональных данных в целях предоставления государственных и муниципальных услуг, а также услуг, которые являются необходимыми и обязательными для предоставления государственных и муниципальных услуг, устанавливается Правительством Российской Федерации.

В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных.

В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

Персональные данные могут быть получены оператором от лица, не

являющегося субъектом персональных данных, при условии предоставления оператору подтверждения наличия оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

Требования к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения, устанавливаются уполномоченным органом по защите прав субъектов персональных данных.

4. ОБРАБОТКА И ХРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ.

4.1. Обработка персональных данных должна осуществляться на основе принципов:

- законности целей и способов обработки персональных данных и добросовестности;
- соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Колледжа;
- соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

4.2. В целях обеспечения прав и свобод человека и гражданина Колледж при обработке персональных данных работника обязан соблюдать следующие общие требования:

- обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве и продвижении по службе, обеспечения личной безопасности, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;
- при определении объема и содержания обрабатываемых персональных данных работника Колледж должен руководствоваться Конституцией Российской Федерации, Трудовым Кодексом и иными федеральными законами.
- сотрудники Колледжа, имеющие доступ к персональным данным работников, имеют право получать только те персональные данные работника, которые необходимы им для выполнения конкретных трудовых

функций.

4.3. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4.3.1. При обработке персональных данных работников Колледж вправе определять способы обработки, документирования, хранения и защиты персональных данных.

4.3.2. Особенности обработки персональных данных без использования средств автоматизации установлены Постановлением Правительства РФ от 15.09.2008 N 687. Как следует из указанного документа, обязательные меры защиты персональных данных в этом случае включают следующие условия:

- в отношении каждой категории персональных данных должно быть возможно определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ;
- раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях;
- соблюдение при хранении материальных носителей условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный к ним доступ (оператор обязан установить перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер).

4.3.3. Документы, содержащие персональные данные работника составляют его личное дело. Личное дело в обязательном порядке включает личную карточку (формы Т-2 для работника). Личное дело хранится уполномоченным лицом на бумажных носителях, а помимо этого может храниться в виде электронных документов. Личное дело пополняется на протяжении всей трудовой деятельности работника.

4.3.4. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

5. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ РАБОТНИКОВ.

5.1. Внутренний доступ (доступ внутри организации). Право доступа к персональным данным работника имеют:

- директор;
- заместители директора;
- отдел кадров;
- бухгалтерия;
- руководители структурных подразделений по направлению деятельности;
- инженер-программист;
- фельдшер в отношении медицинских сведений работников;
- секретарь директора;
- сам работник, носитель данных.

5.2. Внешний доступ. Массовые потребители персональных данных вне организации - государственные и негосударственные функциональные структуры:

- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- страховые агентства;
- военкоматы;
- органы социального страхования;
- пенсионные фонды;
- подразделения муниципальных органов управления.

5.3. Другие организации. Сведения о работающем работнике или уже уволенном могут быть предоставлены другой организации только с письменного запроса на бланке организации с приложением копии заявления работника.

5.4. В случае если Колледжу оказывают услуги юридические и физические лица на основании заключенных договоров (либо иных оснований), и в силу данных договоров они должны иметь доступ к персональным данным работников Колледжа, то соответствующие данные предоставляются Колледжем только после подписания с ними соглашения о неразглашении конфиденциальной информации. В исключительных случаях, исходя из договорных отношений с контрагентом, допускается наличие в договорах пунктов о неразглашении конфиденциальной информации, в том числе

предусматривающих защиту персональных данных работника Колледжа.

5.5. Работник Колледжа, в частности, имеет право:

- получать доступ к своим персональным данным и ознакомление с ними, включая право на безвозмездное получение копии любой записи, содержащей его персональные данные, за исключением случаев, предусмотренных федеральным законом;
- требовать от работодателя исключения или исправления неверных, или неполных персональных данных, а также данных, обработанных с нарушением требований Трудового кодекса РФ или иного федерального закона. При отказе работодателя исключить или исправить персональные данные работника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;
- обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия работодателя при обработке и защите его персональных данных.

6. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ.

6.1. Защита персональных данных работника от неправомерного их использования или утраты обеспечивается Колледжем.

Защите подлежат:

- информация о персональных данных работника;
- документы, содержащие персональные данные работника;
- персональные данные, содержащиеся на электронных носителях.

6.2. Внутренняя защита. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий директора и специалистов Колледжа.

Для защиты персональных данных работников необходимо соблюдать ряд мер:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между работниками;
- рациональное размещение рабочих мест работников, при которых исключалось бы бесконтрольное использование защищаемой информации;

- знание работником требований нормативно-правовых документов по защите персональных данных;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения;
- воспитательная и разъяснительная работа с работниками Колледжа по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- не допускается выдача личных дел работников на рабочие места руководителей структурных подразделений;
- не допускается отвечать на вопросы, связанные с передачей персональных данных по телефону или факсу;
- все данные на электронных носителях должны быть защищены паролем.

6.3. Обеспечение безопасности персональных данных достигается, в частности (ч. 1 ст. 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»):

Инженер-программист обеспечивает защиту персональных данных в компьютерных информационных системах персональных данных:

- 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 учетных записей и системы паролей;
- защита обмена персональными данными при их обработке в информационных системах обеспечивается реализацией соответствующих организационных мер;
- размещение информационных систем, специального оборудования и охрану (опечатывание) помещений, в которых находятся сервера с базами данных, содержащих персональную информацию;
- контроль за предотвращением воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- организация возможности восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- организация обучения лиц, использующих средства защиты информации, применяемых в информационных системах, правилам работы с ними;

- обеспечение учета применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
- контроль соблюдения условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- организация разбирательств и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

6.4. Инженер-программист инициирует организационные, технические и программные мероприятия по обеспечению безопасности персональных данных в информационных системах, для чего взаимодействует с организациями или специалистами, уполномоченными на проведение работ по:

- определению возможных угроз безопасности персональных данных при их обработке в информационных системах, формированию модели угроз, определению класса информационной системы;
- разработке на основе модели угроз системы защиты информационных систем, содержащих персональные данные;
- обеспечение установки и ввода в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;
- проведение проверки готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации.

6.5. Внешняя защита. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося 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 др. Под сторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности Колледжа, посетители, работники других организаций. 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 работников необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;
- пропускной режим;
- технические средства охраны, сигнализации;
- порядок охраны территории, зданий, помещений;
- требования к защите информации при интервьюировании и беседах;
- личные дела хранятся в бумажном виде в папках и находятся в сейфе или в негорючем шкафу, которые запираются на ключ;
- трудовые книжки работников хранятся в сейфе или негорючем шкафу, которые запираются на ключ;
- медицинские книжки работников хранятся в сейфе или в негорючем шкафу, которые запираются на ключ. Ключ хранится у специалиста по кадрам;
- хранение персональных данных работников в бухгалтерии и иных структурных подразделениях Колледжа, сотрудники которых имеют право доступа к персональным данным, осуществляется в порядке, исключающим к ним доступ третьих лиц.

6.6. Сотрудник Колледжа, имеющий доступ к персональным данным работников в связи с исполнением трудовых обязанностей обеспечивает хранение информации, содержащей персональные данные работника, исключающее доступ к ним третьих лиц:

- в отсутствие сотрудника на его рабочем месте не должно быть документов, содержащих персональные данные работников (соблюдение "политики чистых столов");
- при работе специалистов, документы, содержащие персональные данные, могут находиться на рабочих столах или в специальных папках в течение рабочего дня. По окончании рабочего дня данные документы должны убираться в места постоянного хранения, исключающие к ним доступ третьих лиц;
- персональный компьютер, на котором ведется обработка персональных данных, должен быть защищен паролем, а при отсутствии сотрудника на рабочем месте должен блокироваться;
- при уходе в отпуск, служебной командировке и иных случаях длительного отсутствия работника на своем рабочем месте, он обязан передать документы и иные носители, содержащие персональные данные работников

лицу, на которое локальным актом Колледжа (приказом, распоряжением директора) будет возложено исполнение его трудовых обязанностей;

- при увольнении сотрудника, имеющего доступ к персональным данным работников, документы и иные носители, содержащие персональные данные, передаются вновь назначенному на эту должность или другому сотруднику, имеющему доступ к персональным данным по письменному распоряжению директора Колледжа с составлением соответствующего акта.

6.7. Отдел кадров обеспечивает:

- ознакомление сотрудников под роспись с настоящим Положением;

- при наличии иных нормативных актов (приказы, распоряжения, инструкции и т.п.), регулирующих обработку и защиту персональных данных работника, с данными актами также производится ознакомление сотрудника под роспись;

- истребование с сотрудников письменного обязательства о соблюдении конфиденциальности персональных данных работника и соблюдении правил их обработки;

7. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ОБРАБОТКУ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАнных РАБОТНИКА КОЛЛЕДЖА.

7.1. Персональная ответственность – одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

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

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

7.4. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут ответственность в соответствии с федеральными законами:

- дисциплинарную;

- материальную;

- административную;

- гражданско-правовую;

- уголовную.

7.5. Работник, предоставивший работодателю подложные документы или заведомо ложные сведения о себе, несет дисциплинарную ответственность

вплоть до увольнения.

8. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ.


8.1. Настоящее Положение вступает в силу с момента его утверждения директором Колледжа и вводится в действие приказом директора.

8.2. Положение обязательно для всех работников Колледжа, если иные условия не предусмотрены в трудовом договоре работника.

8.3. Директор Колледжа вправе вносить изменения и дополнения в Положение. Работники Колледжа должны быть поставлены в известность о вносимых изменениях и дополнениях за 5 дней до вступления их в силу посредством издания директором приказа и ознакомления с ним всех работников Колледжа.

Разработано:

Юрисконсульт

 Камалова Р.Р.

Согласовано:

Начальник отдела кадров

 Исянгулова М.Ф.

СОГЛАШЕНИЕ
о неразглашении персональных данных работников

Я, _____, паспорт серии _____, номер _____, выданный _____

« ____ » _____ года, понимаю, что получаю доступ к персональным данным работников государственного автономного профессионального образовательного учреждения Стерлитамакский многопрофильный профессиональный колледж. Я также понимаю, что во время исполнения своих обязанностей, мне приходится заниматься сбором, обработкой и хранением персональных данных работников. Я понимаю, что разглашение такого рода информации может нанести ущерб работникам колледжа, как прямой, так и косвенный. В связи с этим я даю обязательство, при работе (сборе, обработке и хранении) с персональными данными работника колледжа соблюдать все требования, описанные в «Положении о порядке обработки и защиты персональных данных работников государственного автономного профессионального образовательного учреждения Стерлитамакский многопрофильный профессиональный колледж».

Я подтверждаю, что не имею права разглашать следующие сведения:

- анкетные и биографические данные (фамилия, имя, отчество (в т.ч. прежние); год, месяц, дата и место рождения, а также иные данные, содержащиеся в удостоверении личности работника);
- образование (данные об образовании работника, наличии специальных знаний или подготовки);
- сведения о трудовом и общем стаже;
- сведения о составе семьи;
- паспортные данные;
- сведения о заработной плате сотрудника;
- сведения о социальных льготах;
- данные о профессии, специальности работника;
- занимаемая должность;
- адрес места жительства;
- мобильный (домашний) телефон;
- состав семьи;
- сведения о доходах работника;
- данные, содержащиеся в трудовой книжке и (или) сведениях о трудовой деятельности работника;
- данные, содержащиеся в документе подтверждающем регистрацию в системе индивидуального (персонифицированного) учета, в том числе в форме электронного документа;
- данные, содержащиеся в документе идентификационный номер налогоплательщика (ИНН) — цифровой код, упорядочивающий учёт налогоплательщиков в Российской Федерации;
- данные, содержащиеся в документах воинского учета (при их наличии);
- документы о состоянии здоровья работника;
- наличие судимостей;
- иные персональные данные, при определении объема и содержания которых работодатель руководствуется настоящим Положением и законодательством РФ.

Я предупрежден(а) о том, что в случае разглашения мной сведений, касающихся персональных данных работника или их утраты я несу ответственность в соответствии с Трудовым кодексом РФ (ст.90).

С «Положением о порядке обработки и защиты персональных данных работников государственного автономного профессионального образовательного учреждения Стерлитамакский многопрофильный профессиональный колледж» ознакомлен(а).

« ____ » _____ 20__ года

Подпись