Приложение №__

к Коллективному договору

ГБПОУ КК КТК

УТВЕРЖДЕНО: Директор ГБПОУ КК «Краснодарский технический колледж»	СОГЛАСОВАНО: Председатель профкома ГБПОУ КК «Краснодарский технический колледж» Профсоюза работников АПК:
Пронько С.В. _____	Костюченко И.В. _____

ПОЛОЖЕНИЕ
о защите персональных данных, организации и проведению работ по обеспечению безопасности персональных данных в государственном бюджетном профессиональном образовательном учреждении Краснодарского края «Краснодарский технический колледж»

1. Термины и определения

Для целей Положения по организации и проведению работ по обеспечению безопасности персональных данных (далее – Положение) используются следующие термины и определения:

1.1. «персональные данные» − любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (п. 1 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ);

1.2. «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 (п. 2 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ);

1.3. «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 (п. 3 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ);
1.4. «распространение персональных данных» − действия, направленные на раскрытие персональных данных работников неопределенному кругу лиц (п. 5 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ);
1.5. «блокирование персональных данных »- временное прекращение обработки персональных данных работников (за исключением случаев, если обработка необходима для уточнения персональных данных) (п. 7 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ);
1.6. «уничтожение персональных данных» - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных работников и (или) в результате которых уничтожаются материальные носители персональных данных работников (п. 8 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ);
1.7. «обезличивание персональных данных» - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному работнику (п. 9 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ) ;
1.8. «информационная система персональных данных» - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
1.9. трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

2. Общие положения

2.1. Целью данного Положения является обеспечение прав и свобод человека и гражданина в отношении их персональных данных путем определения принципов, правил и методов защиты персональных данных от несанкционированного доступа при их обработке в Государственном Бюджетном Профессиональном Образовательном Учреждении «Краснодарский технический колледж » (далее – Колледж,), в том числе при передаче персональных данных третьих лицам.
2.2. Настоящее Положение разработано в соответствии со следующими нормативно-правовыми актами:
2.2.1. Конституцией Российской Федерации;
2.2.2. Гражданским кодексом Российской Федерации;
2.2.3. Трудовым кодексом Российской Федерации;
2.2.4. Федеральным законом от 27.07.2006 г. №152 ФЗ «О персональных данных»;
2.2.5. Постановлением Правительства Российской Федерации от 15.09. 2008 г. №687 «Об утверждении Положения об обязанностях обработки персональных данных, осуществляемых без использования средств автоматизации»,
2.2.6. Постановлением Правительства Российской Федерации от 21.03. 2012 г. №211 « Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных»

2.2.7. Уставом Колледжа;
2.2.8. Коллективным договором Колледжа.
2.3. 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 определено законом.
2.4. Персональные данные, относящиеся к общедоступным, определены в локальных нормативно-правовых актах Колледжа. Далее под персональными данными будем понимать персональные данные, не относящиеся к общедоступным.
2.5. Настоящее Положение является обязательным для исполнения всеми сотрудниками, имеющими допуск к персональным данным сотрудников, абитуриентов, обучающихся, выпускников, и иных лиц, данные которых могут быть переданы Колледжу на законном основании (далее – субъекты персональных данных).
2.6. Настоящее Положение вступает в силу с момента его утверждения директором Колледжа по согласованию с Профкомом.
2.7. Контроль исполнения данного Положения осуществляет директор Колледжа или лицо, назначенное приказом директора Колледжа ответственным за обеспечение безопасности персональных данных в Колледже.

3. Принципы организации работ по защите персональных данных

Для обеспечения защиты персональных данных должны быть реализованы следующие принципы:
3.1. ограничение и регламентация состава работников, функциональные обязанности которых требуют работы с персональными данными;
3.2. строгое избирательное и обоснованное распределение документов и информации между работниками;
3.3. рациональное размещение рабочих мест работников, при котором будет исключено бесконтрольное использование защищаемой информации;
3.4. знание и выполнение работником требований федерального законодательства и локальных нормативно-правовых документов по защите информации и сохранении тайны;
3.5. наличие необходимых условий в помещении для работы с документами, содержащими персональные данные, и базами данных;
3.6. определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;
3.7. организация порядка учета, хранения, уничтожения и передачи конфиденциальной информации;
3.8. своевременное выявление нарушений требований разрешительной системы доступа работниками подразделений;
3.9. возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним или непреднамеренного уничтожения;
3.10. воспитательная и разъяснительная работа с сотрудниками подразделений по предупреждению утраты ценных сведений при работе с персональными данными.

4. Допуск к персональным данным

4.1. К работе с персональными данными, обрабатываемыми в Колледже, должны допускаться только сотрудники, имеющие документально оформленный допуск.
4.2. Лицами, имеющими право давать разрешение на допуск к персональным данным являются: директор, заместители директора, руководители структурных подразделений.
Основополагающими подходами при этом являются:
4.2.1. Директор имеет право давать разрешение на допуск к соответствующей конфиденциальной информации всем сотрудникам;
4.2.2. Заместители директора имеют право давать разрешение на допуск к соответствующим персональным данным всех сотрудников, но в пределах полномочий, возложенных на них директором;
4.2.3. Руководителям подразделений дается право разрешать допуск к персональным данным всех сотрудников своих подразделений по тематике работы подразделений; для осуществления допуска к персональным данным данного подразделения сотрудников других подразделений необходимо разрешение соответствующего заместителя директора;
4.3. Оформление допуска может осуществляться в следующих формах:
4.3.1. составление должностных либо именных списков сотрудников, допускаемых к персональным данным, в обязательном порядке содержащих наименование подразделения, должности и категории сведений (документов), наименования информационных систем, к которым они допускаются;
4.3.2. оформление разрешения непосредственно на документе (носителе информации) в виде резолюции (поручения), адресованного конкретному сотруднику;
4.4. Основанием для допуска к персональным данным служит подписанный директором приказ о приеме на работу на должность, должностная инструкция, а также подписанное обязательство о неразглашении конфиденциальной информации.
4.5. При переводе на другую должность основанием для допуска служит приказ о переводе. В этом случае допуск работника по предыдущей должности прекращается, и он допускается к сведениям по новой должности.
4.6. Основанием для прекращения допуска служит приказ об увольнении либо приказ директора о прекращении допуска данного сотрудника к персональным данным.
4.7. Список лиц, допущенных к обработке персональных данных в рамках своих должностных обязанностей» (далее – Список лиц), утверждается директором Колледжа .
4.8. Сотрудники подразделения, допущенные к работе с персональными данными, должны быть ознакомлены со Списком лиц.
4.9. Копия либо выписка из Списка лиц заверяется и передается в соответствующее структурное подразделение, где хранится у руководителя.
4.10. Доступ к автоматизированным рабочим местам, входящим в состав ИСПДн, осуществляется в соответствии со Списком лиц с использованием ИСПДн. Данный список является именным и включает ФИО сотрудника, подразделение, должность,

сведения, доступ к которым необходим сотруднику, наименование ИСПДн, с которого разрешен самостоятельный доступ к информации.

4.11. До получения доступа к персональным данным все лица, обязанности которых связанны с получением, обработкой и защитой персональных данных, должны подписать обязательство о неразглашении персональных данных.

4.12. Принимаемый на работу сотрудник подписывает обязательство о неразглашении конфиденциальной информации в отделе кадров колледжа.

4.13. Список лиц должен перепечатываться и вновь утверждаться не реже одного раза в год.

4.14. При увольнении сотрудника, имеющего доступ к ИСПДн согласно Списку лиц, отделом кадров немедленно должен быть извещен начальник службы безопасности и ЧС, ответственный за ведение Списка лиц, и ведущий системный администратор, который должен принять меры по блокированию учетной записи увольняемого сотрудника и/или немедленной смене его паролей на доступ к информационным системам.

5. Требования к помещениям

5.1. В помещениях, в которых в рабочее время осуществляется прием посетителей и одновременно ведется обработка персональных данных, должно быть установлено разграничение на 2 зоны: зона А, в которой предусматривается нахождение посетителей и зона Б, в которой предполагается обрабатывать персональные данные.

5.2. Разграничение на зоны должно производиться путем установки физического препятствия, которое затрудняет проникновение к рабочим местам сотрудников в зоне Б.

5.3. В случаях, когда в силу специфики работы установка подобных барьеров невозможна, посетители могут находиться в помещении в специально выделенное для приема посетителей время только при обязательном присутствии сотрудника отдела. Сотрудники на время приема посетителей не осуществляют работу с персональными данными других субъектов. Все документы, содержащие персональные данные, кроме тех, которые не относятся к конкретному посетителю, должны быть убраны в папки или шкафы (сейфы).

5.4. В зоне Б разрешается находиться только сотрудникам, которым в установленном порядке оформлен допуск к соответствующей конфиденциальной информации (персональным данным). Не допускается бесконтрольное нахождение посторонних лиц в помещениях, в которых ведется обработка персональных данных.

5.5. Контроль доступа лиц в помещения зоны Б обеспечивается сотрудниками подразделения.

5.6. В нерабочее время или во время отсутствия сотрудников помещения, в которых ведется обработка персональных данных, должны запираться на ключ. Контроль входа в нерабочее время обеспечивается включением охранной сигнализации.

5.7. Оргтехника должна располагаться таким образом, чтобы обеспечивать невозможность просмотра из зоны А информации выводимой на экраны мониторов и на печать.

5.8. Помещение, где в нерабочее время происходит хранение носителей конфиденциальной информации, должно быть оборудовано охранной и пожарной сигнализацией.
5.9. Окна в помещении оборудуются жалюзи или шторами, которые при работе с персональными данными должны быть закрыты.
5.10. Присутствие обслуживающего персонала Колледжа, в том числе уборка помещений, допускается строго в присутствии хотя бы одного из сотрудников отдела.
5.11. Запрещается изготовление, использование и хранение сотрудниками неучтенных экземпляров ключей. Изготовление дополнительных экземпляров ключей осуществляется путем подачи письменной заявки на имя заместителя директора, ответственного за административно-хозяйственную работу в Колледже. Обязанность по учету и хранению запасных экземпляров ключей возлагается на заместителя директора по УПР. При утере ключа от помещения, где обрабатывается конфиденциальная информация, об этом факте ставится в известность начальник службы безопасности и ЧС, немедленно принимаются меры по замене дверного замка. Заместитель директора по УПР организует работу по выполнению п. 5.2 настоящего положения и несёт ответственность за своевременное выполнение данной работы (согласно п. 5.2) в полном объеме.
5.12. Дополнительные требования к доступу в помещения, в которых ведется обработка персональных данных, могут устанавливаться дополнительными инструкциями о порядке доступа в помещения, в которых ведется обработка персональных данных.

6. Общие требования по обработке персональных данных

6.1. Обработка персональных данных в Колледже должна осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия субъектам персональных данных в осуществлении учебной, научной, преподавательской и иной трудовой деятельности, обеспечения личной безопасности, проведения лечебно-профилактических мероприятий, учета результатов исполнения договорных обязательств, повышения качества деятельности университета, а также наиболее полного исполнения Колледжем обязательств и компетенций в соответствии с Федеральным законом от 29.12.2012 г. № 273-ФЗ "Об образовании в Российской Федерации" (с изменениями и дополнениями).
6.2. При определении объема и содержания, обрабатываемых персональных данных, Колледж и его сотрудники должны руководствоваться федеральными законами и иными локальными нормативно-правовыми актами Колледжа, устанавливающими цель обработки, а также определяющими требования по обеспечению безопасности персональных данных.
6.3. Персональные данные следует получать у самого субъекта персональных данных. Условием обработки персональных данных субъекта персональных данных является получение его письменное согласия.
6.4. Согласие на обработку не требуется получать в случаях, если обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных (трудовой договор, договор на под-

готовку специалиста за полную стоимость обучения), обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных (подразделения Колледж, ответственные за вопросы занятости учащейся молодежи и трудоустройства выпускников); обработка персональных данных осуществляется для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно; обработка персональных данных осуществляется в целях профессиональной деятельности журналиста либо в целях научной, литературной или иной творческой деятельности (штатный фотограф, штатный корреспондент) при условии, что при этом не нарушаются права и свободы субъекта персональных данных №152-ФЗ «О персональных данных», ст.6, п.2)

6.5. Если персональные данные получаются у третьей стороны (например, данные о родителях от абитуриента), то субъект персональных данных должен быть уведомлен об этом заранее. Оператор должен сообщить субъекту наименование и адрес оператора или его представителя, цель обработки персональных данных и ее правовое основание, предполагаемых пользователей персональных данных, установленные Федеральным законом «О персональных данных» права субъекта персональных данных (152-ФЗ «О персональных данных», гл. 4, ст. 18, п.3).

6.6. В случае если предполагается размещать информацию в общедоступных местах (информационные стенды, официальный сайт Колледжа), то необходимо получить от субъекта письменное согласие. (152-ФЗ «О персональных данных», гл. 2, ст. 8, п.1).

6.7. При осуществлении обработки биометрических данных (фотография) следует брать согласие, за исключением случаев, когда обработка осуществляется в связи с осуществлением правосудия, а также в случаях, предусмотренных законодательством Российской Федерации о безопасности, законодательством Российской Федерации об оперативно-розыскной деятельности, законодательством Российской Федерации о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию. (152-ФЗ «О персональных данных», ст. 11).

6.8. Оператор не имеет права получать и обрабатывать персональные данные субъектов персональных данных о его членстве в общественных объединениях или его профсоюзной деятельности, политических, религиозных и иных убеждениях и частной жизни (информация о жизнедеятельности в сфере семейных, бытовых, личных отношений). В случаях, непосредственно связанных с вопросами трудовых отношений и/или обучения субъекта указанные в данном пункте сведения могут быть получены и обработаны оператором только с письменного согласия субъекта.

6.9. Все меры конфиденциальности при обработке персональных данных сотрудника распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

6.10. Не допускается выдача личных дел сотрудников на рабочие места руководителей. Личные дела могут выдаваться на рабочие места только директору, лицу его замещающему, работникам отдела кадров и в исключительных случаях, по письменному разрешению директора - руководителю структурного подразделения (например, при подготовке материалов для аттестации работника).
6.11. При принятии решений, затрагивающих интересы работника, Колледж не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки, без согласия субъекта и уведомления его о юридических последствиях такой обработки.
6.12. Типовые формы документов (в том числе договоров), предполагающих содержание персональных данных, могут согласовываться с юрисконсультом, который проверяет их на соответствие нормативно-правовым актам о персональных данных.
6.13. Запрещается использование обратной стороны бумажных носителей персональных данных для черновиков.
6.14. На рабочем столе работника должен находиться только тот массив документов, с которым в настоящий момент он работает. Другие документы, дела, журналы должны быть убраны в металлические шкафы, сейфы.
6.15. Исполняемые документы не разрешается хранить в россыпи. Их следует помещать в папки, на которых указывается вид производимых с ними действий, например: для подшивки в личные дела, для отправки и т. п., или фамилии граждан, к работе с которыми относятся данные документы.
6.16. В конце рабочего дня все носители, содержащие персональные данные (документы, дела, листы бумаги и блокноты с рабочими записями, инструктивные и справочные материалы) должны быть убраны в металлические шкафы, сейфы.
6.17. При обнаружении нарушения целостности печати либо обнаружении иных признаков несанкционированного доступа в хранилище необходимо немедленно доложить об этом начальнику подразделения и начальнику службы безопасности и ЧС.
7. Общие требования по организации безопасной работы в информационных системах персональных данных

7.1. Директором Колледжа назначается сотрудник, исполняющий обязанности администратора информационной безопасности (далее - системный администратор по защите персональных данных).
7.2. Системный администратор по защите персональных данных действует на основании соответствующего нормативного документа, разработанного и утвержденного руководством Колледжа.
7.3. Руководителями структурных подразделений совместно с ведущим системным администратором определяются технические средства, используемые в ИСПДн, перечень которых утверждается директором Колледжа .
7.4. Работа с информационной системой персональных данных администраторов, пользователей и обслуживающего технические и программные средства персонала должна осуществляться в полном соответствии с требованиями настоящего Поло-

жения, может устанавливаться в соответствии с инструкциями пользователя ИСПДн, администратора ИСПДн, по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств ИСПДн.

7.5. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику Колледжа, допущенному к работе с конкретной ИСПДн, должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться, и работать в системе. Некоторым сотрудникам в случае производственной необходимости могут быть сопоставлены несколько уникальных имен (учетных записей). Использование несколькими сотрудниками при работе с ИСПДн одного и того же имени пользователя («группового имени») запрещено.

7.6. Аутентификация пользователей осуществляется по паролю. Требования к парольной политике определяются Инструкцией пользователя ИСПДн.

7.7. В информационных системах должны применяться лицензионные и сертифицированные средства антивирусной защиты и противодействия вредоносным программным воздействиям. Антивирусная защита осуществляется в соответствии с централизованными настройками агента администрирования.

7.8. Для ИСПДн должен быть назначен администратор, отвечающий за ее сопровождение и обслуживание. Администратором может являться только сотрудник Колледжа .

7.9. Сотрудниками по защите персональных данных должно обеспечиваться резервирование и восстановление информации в ИСПДн. Инструкция резервирования и восстановления утверждается директором. Общие требования к резервированию определяются инструкцией резервного копирования и восстановления из копии ИСПДн.

7.10. При взаимодействии с сетью Интернет должно обеспечиваться противодействие атакам хакеров и распространению спама.

7.11. Порядок подключения и использования ресурсов сети Интернет должен контролироваться подразделениями (сотрудниками) Колледжа, ответственными за обеспечение информационной безопасности. Любое подключение и использование сети Интернет должно быть санкционировано в установленном порядке.

7.12. Использование сети Интернет с автоматизированных рабочих мест, которые входят в состав ИСПДн, ограничивается. В случае крайней необходимости подключение к сети Интернет производится с рабочих мест, входящих в состав ИСПДн, с использованием межсетевого экрана.

7.13. Данные, хранящиеся в ИСПДн, необходимость в обработке которых пропала, передаются на хранение в архив с составлением акта передачи в архив и затем уничтожаются в ИСПДн. Для хранения, комплектования и использования этих данных в архиве может применяться автоматизированный научно-справочный аппарат архива, представляющий собой комплекс электронных справочников (база данных описаний документов), предназначенных для эффективного поиска архивных документов и информации. («Основные правила работы архивов организаций», одобренные решением Коллегии Росархива от 08.04.2011, п. 7.7.1).

7.14. При окончательном уничтожении всех документов, дел, записей в базе данных, содержащих персональные данные, следует уведомить об этом субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, (например, при уничтожении всех документов, дел, записей в базе данных, содержащих данные об окладе, о начислении заработной платы, о составе семьи и т. д.).
7.15. В информационных системах персональных данных должны использоваться средства защиты информации, прошедшие в установленном порядке процедуру оценки соответствия (п.5 Постановления Правительства РФ № 781).
7.16. Сотрудниками ЦИТ должны производиться регулярные обновления операционных систем, системных и прикладных программ, средств защиты информации, антивирусных баз, резервное копирование критичной информации ИСПДн.
7.17. Любые работы с кабельными системами (телефонными линиями, локальными вычислительными сетями, электросетью) должны осуществляться по согласованию с начальником службы безопасности и ЧС Колледжа, а также руководителя Центра информатизации; также – согласовываться с ведущим системным администратором. В разрешении на проведение работ должны быть указаны дата и сроки проведения технических работ, а также стоять подпись начальника службы безопасности и ЧС Колледжа.
7.18. Дополнительные требования к проведению работ по ремонту и обслуживанию средств ИСПДн устанавливаются отдельной инструкцией.
7.19. Обработка персональных данных, содержащихся в информационной системе, либо извлеченных из информационной системы, считается осуществляемой без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека. К таким системам могут относиться электронные документы офисных программных пакетов и другие электронные документы, в которых использование, уточнение, распространение, уничтожение каждой записи о субъекте персональных данных осуществляется человеком и в которых отсутствует обработка с помощью формул, макросов, а также справочники, картотеки, реестры, журналы, дела с заполненными формами типовых документов, и т. п.
7.20. В случае создания или наличия информационных систем персональных данных с использованием средств автоматизации, а также без использования средств автоматизации, содержащих данные более чем о 100 субъектах персональных данных информация, о которых не является общедоступной или обезличенной, необходимо уведомить об этом начальника подразделения и начальника службы безопасности и ЧС Колледжа.

8. Требования к учету носителей персональных данных.

8.1. Учету подлежат студенческие билеты, зачетные книжки, личные и учебные карточки, подлинники и копии документов абитуриентов, личные дела студентов и

работников, справки, заявления, расчетные листки, договоры, контракты, документы, содержащие финансовые сведения.
8.2. Черновики и варианты документов не учитываются и уничтожаются работником с отражением факта уничтожения в учетных формах за подписью работника, уничтожившего носитель.
8.3. В информационных системах персональных данных, либо средствах защиты информации должен быть обеспечен контроль вывода информации на бумажные носители, контроль доступа к файлам ИСПДн и контроль копирования файлов на отчуждаемые носители.
8.4. Электронные отчуждаемые носители персональных данных (флэш-накопители, дискеты, оптические накопители и т. п.) подлежат учету в журнале учета отчуждаемых электронных носителей. Журнал хранится у начальника службы безопасности и ЧС Колледжа.
8.5. Запрещается использовать для хранения, переноса персональных данных неучтенные электронные носители.
8.6. Сдаваемые электронные отчуждаемые носители персональных данных многократного пользования должны быть подвергнуты ответственным лицом процедуре уничтожения остаточной информации и храниться в сейфе до необходимости повторной выдачи.
8.7. Входящие и исходящие конфиденциальные документы в обязательном порядке регистрируются в отделе служебной документации. На документах, содержащих конфиденциальную информацию и направляемых в другие организации, проставляется пометка «Конфиденциально».
8.8. Все документы, передаваемые во внешние организации, должны иметь бумажные или электронные копии, хранящиеся в отделе служебной документации.
8.9. Выдача персонифицированных документов, содержащих не общедоступные персональные данные, (в том числе справки, расчетные листки, дипломы, трудовые книжки) производится при предъявлении паспорта лично субъекту персональных данных, либо по нотариально заверенной доверенности.
8.10. Документы по просьбе субъекта персональных данных могут быть отправлены на верифицированный адрес субъекта персональных данных заказным письмом. Верифицированным является адрес, сообщенный непосредственно субъектом персональных данных.

9. Требования к организации хранения носителей персональных данных

9.1. Хранение персональных данных должно происходить в порядке, исключающем их утрату и/или их неправомерное использование.
9.2. Архивные дела, конфиденциальные документы, учетные журналы и книги учета хранятся в рабочее и нерабочее время в запирающихся шкафах либо специально выделенных для хранения помещениях с регламентированным доступом (далее - хранилища).
9.3. Трудовые книжки и иные важные документы хранятся в металлическом шкафу, сейфе либо выделенном помещении с регламентированным доступом. К важным документам следует относить документы, утрата которых либо утечка содер-

жащейся в них информации способна привести к негативным последствиям для субъекта персональных данных (данные о заработной плате, паспортные данные и тому подобное).

9.4. Материалы, связанные с анкетированием, тестированием, проведением собеседований относятся к документам, содержащим персональные данные высокой степени конфиденциальности, и помещаются в отдельное дело.

9.5. При отзыве согласия субъекта персональных данных его данные передаются на архивное хранение в архив Колледжа. Организация хранения, комплектования, учета и использования содержащих архивных документов должна происходить в соответствии с законодательством об архивном деле в Российской Федерации.

9.6. Изъятие данных из архива с целью совершения операций, не относящихся к хранению (например, для создания новых документов, для составления справок, выписок), считается возобновлением обработки персональных данных. При этом проверяется срок действия согласия субъекта и при необходимости берется повторное согласие.

9.7. В каждом отделе, ведущем обработку персональных данных, должны быть назначены сотрудники, ответственные за хранение документов, содержащих персональные данные, а также должны быть выделены хранилища для хранения закрепленных за сотрудниками документов, дел.

9.8. Документы выдаются для работы в начале дня исполнителям сотрудником, ответственным за хранение документов и конце дня должны быть сданы и заперты в хранилище.

9.9. Ответственными за организацию и контроль хранения носителей, содержащих персональные данные, в подразделении являются начальник подразделения и его заместитель на время отсутствия начальника.

9.10. Печати, штампы, бланки документов, ключи от хранилищ хранятся только в металлическом шкафу (сейфе) заместителя директора колледжа по УПР.

10. Общие требования к уничтожению персональных данных.

10.1. Уничтожение документов, содержащих персональные данные, производится по достижении целей их обработки согласно номенклатуре дел и документов.

10.2. Уничтожению подлежат документы, не подлежащие архивному хранению, а также не имеющие научно-исторической ценности или иного практического значения.

10.3. Уничтожение производится по мере необходимости в зависимости от объемов, накопленных для уничтожения документов.

10.4. Накапливаемые для уничтожения документы, копии документов, черновики, содержащие персональные данные должны храниться в отдельном деле или другом контейнере, доступ к которому физически ограничен.

10.5. Содержащие персональные данные документы, копии и черновики документов при отсутствии надобности должны уничтожаться в специальной бумагорезальной машине (шредере) или другим способом, значительно затрудняющим восстановление информации.

10.6. Запрещается выбрасывать в мусор не уничтоженные носители персональных данных или носители, не прошедшие процедуру стирания информации.

11. Общие требования по передаче персональных данных.

11.1. При передаче персональных данных субъекта Колледж должен соблюдать следующие требования:

11.1.1. не сообщать персональные данные субъекта третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, установленных федеральным законом;

11.1.2. не сообщать персональные данные субъекта в коммерческих целях без его письменного согласия;

11.1.3. предупреждать лиц, получающих персональные данные субъекта о том, что эти данные могут быть использованы лишь в тех целях, для которых они сообщены, и требовать от этих лиц подтверждения соблюдения этого правила. Лица, получающие персональные данные субъекта, обязаны соблюдать режим конфиденциальности. Данное Положение не распространяется на обмен персональными данными субъекта в порядке, установленном федеральными законами;

11.1.4. разрешать допуск к персональным данным субъекта только специально уполномоченным лицам, определенным приказом по Колледжу, при этом указанные лица должны иметь право получать только те персональные данные субъекта, которые необходимы для выполнения конкретных функций;

11.1.5. не запрашивать информацию о состоянии здоровья субъекта, за исключением тех сведений, которые относятся к вопросу о возможности выполнения субъектом своих функции;

11.2. При передаче персональных данных субъекта потребителям (в том числе и в коммерческих целях) за пределы организации Колледж не должен сообщать эти данные третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника или в случаях, установленных федеральным законом. Не допускается отвечать на вопросы, связанные с передачей персональной информации, с использованием открытых каналов связи, по телефону или факсу.

11.3. Транспортировка, передача носителей персональных данных должна происходить в порядке, исключающем случайную утрату носителей или утечку персональных данных (например, папки, портфели, кейсы).

11.4. На основании федерального законодательства персональные данные субъектов могут запрашиваться и передаваться в налоговые органы (УФНС РФ по г. Краснодару), органы статистики (в обезличенном виде), пенсионные фонды (Управление пенсионного фонда по КК), отделы военкомата КК, в органы социальной защиты (Управление социальной защиты граждан по г.Краснодару), в судебные (городской суд, районный суд, Верховный суд, арбитражный суд, Конституционный суд, мировой суд), правоохранительные (прокуратура, УВД, МВД) и другие органы в пределах их полномочий, при предъявлении их сотрудниками соответствующих документов.

11.5. Единоразовую передачу персональных данных граждан на основании мотивированного запроса вышеобозначенным государственным структурам следует проводить с разрешения директора, которое оформляется в виде приказа директора о передаче персональных данных конкретным сотрудникам вышеобозначенных органов. Передача информации, либо ознакомление с ней фиксируется в соответствующем журнале.
11.6. Порядок передачи персональных данных между сотрудниками в пределах Колледжа:
11.6.1. Передача персональных данных может осуществляться только между сотрудниками, имеющими допуск к персональным данным.
11.6.2. Дела и документы выдаются работникам других подразделений под роспись в журнале учета. При возврате дела тщательно проверяется сохранность документов, отсутствие повреждений, включения в дело других документов или подмены документов.
11.6.3. При смене работников, ответственных за учет и хранение документов, содержащие персональные данные, составляется в произвольной форме акт их приема-передачи, который утверждается директором или начальником отдела, которому принадлежат работники.
11.6.4. Работник, не имеющий допуска, имеет право знакомиться с документами, содержащими только его персональные данные (карточкой формы Т-2, трудовой книжкой, приказами и заявления, содержащими его персональные данные). Ознакомление с этими документами должно производиться таким образом, чтобы избежать их утраты.
11.7. Запрещается выносить документы, содержащие персональные данные субъекта, из служебных помещений для работы с ними на дому, в гостиницах и т. д. В необходимых случаях директор может разрешить исполнителям или секретарю-референту вынос из здания таких документов (в соответствующих кейсах, чемоданах, портфелях) для их согласования, подписи и т. п. в организациях, находящихся в пределах города.
11.8. Лицам, выезжающим на другие территории, запрещается иметь при себе в пути следования документы и машинные носители, содержащие персональные данные. Эти материалы должны быть направлены заранее в адрес организации по месту командировки сотрудника заказными или ценными почтовыми отправлениями.
11.9. При передаче персональных данных на обработку третьим лицам (например, поликлиникам) с ними должен заключаться договор, существенным условием которого является обязанность обеспечения указанным лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке.

12. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными.

12.1. Персональная ответственность – одно из главных требований к организации функционирования системы защиты персональных данных и обязательное условие обеспечения эффективности этой системы.

12.2. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.
12.3. Руководитель, разрешающий доступ сотрудника к персональным данным, несет персональную ответственность за обоснованность данного решения.
12.4. Каждый сотрудник организации, получающий для работы документ, содержащий персональные данные, несет личную ответственность за сохранность носителя и конфиденциальность информации.
12.5. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.
12.6. Неправомерность деятельности органов государственной власти и организаций по сбору и использованию персональных данных может быть установлена в судебном порядке.
12.7. Лица, ответственные за реализацию системы защиты информации, несут ответственность за достаточность и эффективность применяемых организационных и технических мер.
12.8. Каждый сотрудник, работающий в помещениях с персональными данными, несет персональную ответственность, за исключением НСД к носителю, а также за конфиденциальность содержащейся на нем информации.
12.9. Лица, работающие с персональными данными, несут ответственность за несоблюдение ими требований документов, регламентирующих организацию и обеспечение безопасности персональных данных при их обработке, в соответствии с законодательством Российской Федерации.
