УТВЕРЖДАЮ
Директор ГАПОУ РС (Я) «ЮЯТК»
_____/Подмазкова И.Ю./
«13» марта 2019 г.

ПОЛОЖЕНИЕ
О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ И ОБУЧАЮЩИХСЯ ГОСУДАРСТВЕННОМ АВТОНОМНОМ ПРОФЕССИОНАЛЬНОМ ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ РЕСПУБЛИКИ (САХА) ЯКУТИЯ «ЮЖНО-ЯКУТСКИЙ ТЕХНОЛОГИЧЕСКИЙ КОЛЛЕДЖ»

Введено приказом директора колледжа от 13.03.2019 г. №01-06/73

Вводится взамен утратившего силу, утвержденного Приказом директора от 18.02.2013 г. №32

г. Нерюнгри 2019 г

1. Назначение и область применения

1.1. Положение о защите персональных данных работников и обучающихся в Государственном автономном профессиональном образовательном учреждении Республики (Саха) Якутия «Южно-Якутский технологический колледж» (далее - Положение, Колледж, Образовательная организация) разработано с целью защиты информации, относящейся к личности и личной жизни работников и обучающихся образовательной организации, от несанкционированного доступа, неправомерного их использования или утраты.

1.2. Настоящее положение устанавливает порядок приема, поиска, сбора, систематизации, накопления, хранения, уточнения, обновления, изменения, использования, распространения (в том числе передачи), обезличивания, блокирования, уничтожения, учета документов, содержащих сведения, отнесенные к персональным данным работников и обучающихся в образовательной организации с использованием средств автоматизации или без использования таких средств.

2. Нормативные ссылки и общие положения

2.1. При разработке настоящего Положения использованы следующие нормативные документы:

- п. 1 ст. 23, ст. 24 Конституции Российской Федерации;
- гл. 14 Трудового кодекса Российской Федерации;
- Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;
- Федеральный закон от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных»;
- Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ Рособрнадзора от 01.03.2019 № 214 «Об утверждении Правил осуществления в Федеральной службе по надзору в сфере образования и науки внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами Федеральной службы по надзору в сфере образования и науки» и иными нормативными актами, действующими на территории Российской Федерации.

2.2. Настоящее Положение обязательно для исполнения всеми обучающимися и работниками, участвующими в обеспечении реализации образовательного процесса в колледже.

3. Понятие и состав персональных данных

3.1. 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);

- 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;

- 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;

- 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;

- документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

3.2. К персональным данным работника, получаемым работодателем и подлежащим хранению у работодателя в порядке, предусмотренном действующим законодательством и настоящим Положением, относятся следующие сведения, содержащиеся в личных делах работников:

- фамилия, имя, отчество (в т.ч. прежние), дата и место рождения;

- паспортные данные или данные иного документа, удостоверяющего личность работника;

- адрес места жительства (по паспорту и фактический) и дата регистрации по месту жительства или по месту пребывания;

- номера телефонов (мобильного и домашнего), в случае их регистрации на имя субъекта персональных данных или по адресу его места жительства (по паспорту);

- сведения о номере и серии страхового свидетельства государственного пенсионного страхования;

- сведения об идентификационном номере налогоплательщика (при его наличии у работника);

- сведения о воинском учете военнообязанных лиц и лиц, подлежащих призыву на военную службу (серия, номер, дата выдачи, наименование органа, выдавшего военный билет, военно-учетная специальность, воинское звание, категория запаса, категория годности к военной службе, данные о принятии/снятии на(с) учет(а), сведения о выдаче мобилизационного предписания);

- сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки (серия, номер, дата выдачи диплома, свидетельства, аттестата или другого документа об окончании образовательного учреждения, наименование и местоположение образовательного учреждения, дата начала и завершения обучения, факультет или отделение, квалификация и специальность по окончании образовательного учреждения, ученая степень, ученое звание, владение иностранными языками и другие сведения);

- сведения о повышении квалификации и переподготовке (серия, номер, дата выдачи документа о повышении квалификации или о переподготовке, наименование и местоположение образовательного учреждения, дата начала и завершения обучения, квалификация и специальность по окончании образовательного учреждения и другие сведения);

- сведения о трудовой деятельности (данные о трудовой занятости на текущее время с полным указанием должности, подразделения, наименования, адреса и телефона организации, а также реквизитов других организаций с полным наименованием занимаемых ранее в них должностей и времени работы в этих организациях, а также другие сведения);

- сведения о номере, серии и дате выдачи трудовой книжки (вкладыша в нее) и записях в ней;

- материалы по аттестации работников;

- материалы по расследованию и учету профессиональных заболеваний и несчастных случаев на производстве в соответствии с Трудовым кодексом Российской Федерации, другими федеральными законами;

- сведения о государственных и ведомственных наградах, почетных и специальных званиях, поощрениях (в том числе наименование или название награды, звания или поощрения, дата и вид нормативного акта о награждении или дата поощрения)

- сведения о наличии (отсутствии) судимости и (или) факта уголовного преследования либо прекращения уголовного преследования по реабилитирующим основаниям, выданные в порядке и по форме, которые устанавливаются федеральным органом исполнительной власти;

- сведения из страховых полисов обязательного (добровольного) медицинского страхования;

- сведения о семейном положении (состояние в браке, данные свидетельства о заключении брака, фамилия, имя, отчество супруга (и), паспортные данные супруга (и), степень родства, фамилии, имена, отчества и даты рождения других членов семьи, данные свидетельств о рождении детей);

- сведения о состоянии здоровья детей и других родственников;

- сведения о состоянии здоровья (сведения об инвалидности, о беременности и т.п.);

- содержание и реквизиты трудового договора;

- сведения о заработной плате (номера счетов для расчета с работниками, данные по окладу, надбавкам, премиям, материальной помощи, единовременным выплатам, иным выплатам, налогам);

- сведения о временной нетрудоспособности;

- сведения о приеме, переводах, увольнении работника;

- сведения о социальных льготах и о социальном статусе (серия, номер, дата выдачи, основание выдачи, наименование органа, выдавшего документ, являющийся основанием для предоставления льгот и статуса);

- видео- и фотоизображения, полученные с камер наружного и внутреннего наблюдения, а также с концертов, массовых мероприятий, размещаемые на официальном сайте образовательной организации, в прессе, в государственных информационных системах (ФИС ЕГЭ, ФРДО и т.д.);

- иные сведения, которые с учетом специфики работы и в соответствии с законодательством Российской Федерации должны быть предъявлены работником при заключении трудового договора или в период его действия (включая медицинские заключения, предъявляемые работником при прохождении обязательных предварительных и периодических медицинских осмотров).

3.3. К персональным данным обучающихся, получаемым образовательной организацией и подлежащим хранению в образовательной организации в порядке, предусмотренном действующим законодательством и настоящим Положением, относятся следующие сведения, содержащиеся в личных делах обучающихся:

- фамилия, имя, отчество (в т.ч. прежние), дата и место рождения;

- паспортные данные или данные иного документа, удостоверяющего личность обучающегося;

- адрес места жительства (по паспорту и фактический) и дата регистрации по месту жительства или по месту пребывания;

- сведения о составе семьи;

- паспортные данные родителей (законных представителей) обучающегося;

- сведения об образовании (серия, номер, дата выдачи диплома, свидетельства, аттестата или другого документа об окончании образовательного учреждения, наименование и местоположение образовательного учреждения, дата начала и завершения обучения и другие сведения);

- сведения из страховых полисов обязательного (добровольного) медицинского страхования;

- сведения о состоянии здоровья (сведения об инвалидности, о наличии хронических заболеваний, медицинское заключение об отсутствии противопоказаний для обучения в образовательном учреждении конкретного вида и типа, о возможности изучения предметов, представляющих повышенную опасность для здоровья и т.п.);

- сведения, подтверждающие права на дополнительные гарантии и компенсации по определенным основаниям, предусмотренным законодательством (родители-инвалиды, неполная семья, ребенок-сирота и т.п.);

- видео- и фотоизображения, полученные с камер наружного и внутреннего наблюдения, а также с концертов, массовых мероприятий, размещаемые на официальном сайте образовательной организации, в прессе, в государственных информационных системах (ФИС ЕГЭ, ФРДО и т.д.);

- иные сведения, содержащие персональные данные (в том числе сведения, необходимые для предоставления обучающемуся гарантий и компенсаций, установленных действующим законодательством).

Родители (законные представители) могут сообщить иные сведения, с которыми считают нужным ознакомить работников образовательной организации.

3.4. 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 законодательством.

3.5. Настоящее Положение утверждается и вводится в действие приказом директора образовательной организации и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным сотрудников и (или) обучающихся в образовательной организации. Все работники образовательной организации должны быть ознакомлены под роспись с данным положением и изменениями к нему.

4. Основные условия проведения обработки персональных данных

4.1. Колледж определяет объем, содержание обрабатываемых персональных данных работников и обучающихся, руководствуясь действующим законодательством.

4.2. Обработка персональных данных работников осуществляется в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, а также обеспечения личной безопасности работников, сохранности имущества, контроля количества и качества выполняемой работы.

Обработка персональных данных обучающихся может осуществляться в целях обеспечения соблюдения законов и иных нормативных правовых актов; содействия обучающимся в обучении, трудоустройстве; обеспечения их личной безопасности; контроля качества обучения и обеспечения сохранности имущества.

4.3. Персональные данные работника предоставляются работником, за исключением случаев, предусмотренных федеральным законом. Если персональные данные работника возможно получить только у третьей стороны, то работодатель обязан заранее уведомить об этом работника и получить его письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

4.4. Персональные данные несовершеннолетнего обучающегося предоставляются его родителями (законными представителями). Если персональные данные обучающегося возможно получить только у третьей стороны, то родители (законные представители) обучающегося должны быть уведомлены об этом заранее. От них должно быть получено письменное согласие на получение персональных данных от третьей стороны. Родители (законные представители) обучающегося должны быть проинформированы 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.

4.5. Обработка персональных данных осуществляется с письменного согласия субъектов персональных данных по форме, установленной колледжем.

4.6. Объем и характер обрабатываемых персональных данных, способы обработки персональных данных должны соответствовать целям обработки персональных данных.

4.7. Колледж не имеет права получать и обрабатывать персональные данные работника, обучающегося о его политических, религиозных и иных убеждениях и частной жизни без письменного согласия работника, родителей обучающегося.

Колледж не имеет права получать и обрабатывать персональные данные работника, обучающегося о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

Колледж вправе осуществлять сбор, передачу, уничтожение, хранение, использование информации о политических, религиозных, других убеждениях и частной жизни, а также информации, нарушающей тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений:

- работника только с его письменного согласия или на основании судебного решения;

- обучающегося только с его письменного согласия, письменного согласия родителей (законных представителей) несовершеннолетнего обучающегося или на основании судебного решения.

4.8. Следует обеспечивать точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Уполномоченные должностные лица должны принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

5. Хранение, обработка и использование персональных данных

5.1. Персональные данные работников и обучающихся колледжа хранятся на бумажных и электронных носителях, в специально предназначенных для этого помещениях, в местах, обеспечивающих защиту от несанкционированного доступа.

5.2. В процессе хранения персональных данных работников и обучающихся в колледже должны обеспечиваться:

- требования нормативных документов, устанавливающих правила хранения конфиденциальных сведений;

- сохранность имеющихся данных, ограничение доступа к ним, в соответствии с законодательством Российской Федерации и настоящим Положением;

- контроль за достоверностью и полнотой персональных данных, их регулярное обновление и внесение по мере необходимости соответствующих изменений.

5.3. Право доступа к персональным данным работников и обучающихся в колледже имеют:

директор;

- главный бухгалтер;
- заместитель директора по учебно-производственной работе;
- заместитель директора по социально-воспитательной работе;
- заместитель директора по административно-хозяйственной работе;
- начальник отдела автоматизированных систем управления.

5.4. Право доступа только к персональным данным работников имеют:

- начальник отдела кадров;
- специалист по кадрам.

5.5. Право доступа к персональным данным обучающихся имеют:

- заведующий учебной частью;
- заведующий отделением;
- заведующий методическим отделом;
- заведующий отделом Многофункциональный центр прикладных квалификаций;

- заведующий отделом дополнительного профессионального образования и управления проектной деятельностью;
- заведующий отделом инклюзивного профессионального образования;
- заведующий отделом по формированию контингента студентов;
- заведующий отделом по внеучебной работе;
- методист;
- специалист по учебно-методической работе;
- тьютор отделения;
- педагог-психолог;
- социальный педагог;
- педагог-дополнительного образования;
- лаборант.

5.6. Лица, имеющие доступ к персональным данным обязаны использовать персональные данные работников и обучающихся лишь в целях, для которых они были предоставлены:

Персональные данные работников используются для целей, связанных с выполнением трудовых функций. Администрация колледжа использует персональные данные, в частности, для решения вопросов аттестации, формирования учебного плана, составления отчетов, формирования различных баз данных, продвижения работников по службе, установления размера зарплаты. На основании персональных данных решается вопрос о допуске работника к информации, составляющей служебную тайну.

Персональные данные обучающихся используются для целей, связанных с осуществлением учебно-воспитательного процесса. Администрация и педагогические работники колледжа использует персональные данные для формирования групп, составления учебного плана, составления отчетов, формирования различных баз данных, для возможности поддерживать связь с родителями (законными представителями), учета особенностей обучающихся при его обучении и воспитании.

При принятии решений, затрагивающих интересы работника, администрация не имеет права основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или электронного получения.

Работодатель не вправе принимать решения, затрагивающие интересы работника, основываясь на данных, допускающих двоякое толкование. В случае если на основании персональных данных невозможно достоверно установить какой-либо факт, работодатель должен предложить работнику представить письменные разъяснения.

5.7. Персональные данные работника отражаются в личной карточке работника (форма Т-2), которая заполняется после издания приказа о его приеме на работу. Личные дела работников хранятся в бумажном виде в папках в специальном сейфе.

Персональные данные обучающегося отражаются в его личном деле, которое заполняется после издания приказа о его зачисления в колледж. Личные дела обучающихся в алфавитном порядке формируются в папках групп, которые хранятся в специально оборудованном шкафу.

5.8. Отдельные сведения об обучающихся содержатся в журнале аудиторных занятий, куда заносятся руководителем учебной группы. Журналы аудиторных занятий хранятся в учебной части.

5.9. Персональные данные обучающихся могут также храниться в электронном виде в локальной компьютерной сети. Право полного доступа к электронным базам данных, содержащим персональные данные обучающихся, имеет администрация. Остальные

педагогические работники имеют доступ только к той информации, которая им необходима в пределах исполнения их должностных обязанностей.

5.10. Копировать и делать выписки из персональных данных обучающихся разрешается исключительно в служебных целях с письменного разрешения родителей (законных представителей) и директора колледжа.

5.11. Видео- и фотоизображения работников и обучающихся, полученные на концертах, массовых мероприятиях, допускается размещать на официальном сайте колледжа, в прессе, в государственных информационных системах (ФИС ЕГЭ, ФРДО и т.д.).

5.12. Видео- и фотоизображения, полученные с камер наружного и внутреннего наблюдения, хранятся в электронном виде на отдельном компьютере, подключенном к системе видеонаблюдения, и имеют ограниченный доступ лиц. Работники и обучающиеся информируются о ведении видеонаблюдения путем размещения соответствующих информационных указателей в местах ведения видеонаблюдения.

6. Требования к защите персональных данных при их обработке в информационных системах персональных данных

6.1. Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы, определенные в соответствии с частью 5 статьи 19 Федерального закона «О персональных данных».

6.2. Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

6.3. Безопасность персональных данных при их обработке в информационной системе обеспечивает оператор этой системы, который обрабатывает персональные данные (далее - оператор), или лицо, осуществляющее обработку персональных данных по поручению оператора на основании заключаемого с этим лицом договора (далее - уполномоченное лицо). Договор между оператором и уполномоченным лицом должен предусматривать обязанность уполномоченного лица обеспечить безопасность персональных данных при их обработке в информационной системе.

6.4. Выбор средств защиты информации для системы защиты персональных данных осуществляется оператором в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю во исполнение части 4 статьи 19 Федерального закона «О персональных данных».

6.5. Информационная система является информационной системой, обрабатывающей специальные категории персональных данных, если в ней обрабатываются персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных.

Информационная система является информационной системой, обрабатывающей биометрические персональные данные, если в ней обрабатываются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для

установления личности субъекта персональных данных, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных.

Информационная система является информационной системой, обрабатывающей общедоступные персональные данные, если в ней обрабатываются персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона «О персональных данных».

Информационная система является информационной системой, обрабатывающей иные категории персональных данных, если в ней не обрабатываются персональные данные, указанные в абзацах первом - третьем настоящего пункта.

Информационная система является информационной системой, обрабатывающей персональные данные сотрудников оператора, если в ней обрабатываются персональные данные только указанных сотрудников. В остальных случаях информационная система персональных данных является информационной системой, обрабатывающей персональные данные субъектов персональных данных, не являющихся сотрудниками оператора.

6.6. Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

6.7. Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится оператором с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Федерального закона «О персональных данных», и в соответствии с нормативными правовыми актами, принятыми во исполнение части 5 статьи 19 Федерального закона «О персональных данных».

6.8. При обработке персональных данных в информационных системах устанавливаются 4 уровня защищенности персональных данных.

6.9. Необходимость обеспечения 1-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

6.10. Необходимость обеспечения 2-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает биометрические персональные данные;

г) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

д) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

е) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

6.11. Необходимость обеспечения 3-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные сотрудников оператора или общедоступные персональные данные менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

г) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает биометрические персональные данные;

д) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

6.12. Необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

6.13. Для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечение сохранности носителей персональных данных;

в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

6.14. Для обеспечения 3-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных пунктом 13 настоящего документа, необходимо, чтобы было назначено должностное лицо (работник), ответственный за обеспечение безопасности персональных данных в информационной системе.

6.15. Для обеспечения 2-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных пунктом 14 настоящего документа, необходимо, чтобы доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.

6.16. Для обеспечения 1-го уровня защищенности персональных данных при их обработке в информационных системах помимо требований, предусмотренных пунктом 15 настоящего документа, необходимо выполнение следующих требований:

а) автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе;

б) создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности.

6.17. Контроль за выполнением настоящих требований организуется и проводится оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые оператором (уполномоченным лицом).

7. Передача персональных данных

7.1. При передаче персональных данных работников и обучающихся колледжа другим юридическим и физическим лицам необходимо соблюдать следующие требования:

- персональные данные работника, обучающегося не могут быть сообщены третьей стороне без письменного согласия работника, родителей (законных представителей) несовершеннолетнего обучающегося, за исключением случаев, когда это необходимо для предупреждения угрозы жизни и здоровью работника, обучающегося, а также в случаях, установленных законодательством;

- лица, получающие персональные данные работника, обучающегося должны предупреждаться о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены. Колледж должен требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, обучающегося обязаны соблюдать режим конфиденциальности. Данное положение не распространяется на обмен персональными данными работников в порядке, установленном законодательством;

- передача персональных данных работника, обучающегося его представителям может быть осуществлена в установленном действующим законодательством порядке только в том объеме, который необходим для выполнения указанными представителями их функций;

- необходимо предупреждать лиц, получающих персональные данные субъекта персональных данных, о том, что эти данные должны использоваться только в целях, для которых они сообщены, и требовать от этих лиц подтверждения о соблюдении требований;

- следует не отвечать на вопросы, связанные с передачей персональных данных по телефону или факсу.

7.2. Опубликование и распространение персональных данных допускается в случаях, установленных законодательством.

8. Обязанности, права и ответственность сторон

8.1. Лица, ответственные за организацию обработки персональных данных в колледже, обязаны:

- осуществлять внутренний контроль за соблюдением колледжем как оператором персональных данных и его сотрудниками законодательства РФ о персональных данных, в том числе требований к защите персональных данных;

- доводить до сведения сотрудников колледжа положения законодательства РФ о персональных данных, локальных нормативных актов по вопросам обработки персональных данных, требований к защите персональных данных;

- организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

8.2. В целях обеспечения защиты персональных данных, хранящихся в колледже, работники, родители (законные представители) несовершеннолетнего обучающегося, имеют право:

- получать полную информацию о своих персональных данных и их обработке;

- свободного бесплатного доступа к своим персональным данным, включая право на получение копии любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральными законами. Получение указанной

информации о своих персональных данных возможно при личном обращении работника, родителей (законных представителей) к ответственному за организацию и осуществление хранения персональных данных работников;

- требовать об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований действующего законодательства. Указанное требование оформляется письменным заявлением работника на имя руководителя колледжа;

- требовать об извещении колледжем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обучающегося обо всех произведенных в них исключениях, исправлениях или дополнениях;

- обжаловать в суде любые неправомерные действия или бездействия колледжа при обработке и защите его персональных данных.

8.3. В целях обеспечения достоверности персональных данных работники обязаны:

- при приеме на работу в колледж представлять уполномоченным работникам колледжа достоверные сведения о себе в порядке и объеме, предусмотренном законодательством РФ;

- в случае изменения персональных данных работника: фамилия, имя, отчество, адрес места жительства, паспортные данные, сведения об образовании, состоянии здоровья (вследствие выявления в соответствии с медицинским заключением противопоказаний для выполнения работником его должностных, трудовых обязанностей и т.п.) сообщать об этом;

8.4. В целях обеспечения достоверности персональных данных обучающихся:

- обучающиеся, родители, законные представители несовершеннолетних обучающихся при приеме в колледж предоставляют уполномоченным работникам колледжа достоверные сведения о себе и своих несовершеннолетних детях;

- в случае изменения сведений, составляющих персональные данные обучающегося, обучающийся, родители (законные представители) несовершеннолетнего обучающегося обязаны в течение месяца сообщить об этом уполномоченному работнику колледжа.

8.5. Иные права, обязанности, действия сотрудников, в трудовые обязанности которых входит обработка персональных данных работника, определяются также должностными инструкциями.

8.6. Лица, виновные в нарушении норм, регулирующих получение, обработку, хранение и защиту персональных данных, привлекаются к ответственности в соответствии с законодательством РФ.

8.7. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, установленном федеральными законами.

9. Порядок внесения изменений и дополнений в настоящее положение

9.1. По мере необходимости приказом директора в Положение вносятся изменения и дополнения;

9.2. Копия приказа о внесении изменений и дополнений в Положение направляется всем заинтересованным подразделениям и должностным лицам и хранится вместе с основным текстом Положения;

9.3. В Положение допускается вносить не более пяти изменений и дополнений, после чего оно подлежит пересмотру;

9.4. Изменения оформляются на отдельном листе с обязательным указанием регистрационного номера приказа;

9.5. Положение подлежит обязательному пересмотру один раз в пять лет.

9.6. Настоящее положение считается отмененным, если введена в действие его новая редакция.

10. Контроль над выполнением требований настоящего положения

Контроль над выполнением требований настоящего положения осуществляет заместитель директора по учебно-производственной работе.

Лист учета изменений

№ п/п	Дата внесения изменений	Номера листов	Документ, на основании которого внесено изменение	Краткое содержание изменения	Ф.И.О.,	подпись