

ПРИНЯТО:

Советом техникума

Протокол № 2

Секретарь Совета техникума

Евдокимова Н.А.

«10» мая 2023 г.

УТВЕРЖДЕНО:

Приказом директора ГБПОУ «КПГТ»

от 11.05.2023г. № 01-03/343уч

Директор ГБПОУ «КПГТ»

Т.А. Гвоздева

«11» мая 2023 г.



ПОЛОЖЕНИЕ О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ И ОБУЧАЮЩИХСЯ ГБПОУ «КАСЛИНСКИЙ ПРОМЫШЛЕННО-ГУМАНИТАРНЫЙ ТЕХНИКУМ»

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Положение о защите персональных данных (далее – Положение) определяет понятие и состав персональных данных, требования к обработке, хранению и защите персональных данных работника, необходимых в связи с трудовыми отношениями.

1.2. Положение основано на следующих нормативных документах:

– Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных»);

– Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ;

– Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Устав техникума и иные локальные нормативные акты.

1.3. Положение вступает в силу с момента его утверждения директором техникума (далее – Техникум) и действует до замены его новым Положением.

1.4. В Положении используются следующие основные понятия:

– персональные данные работника – любая информация, относящаяся к определенному или определяемому на основании такой информации работнику, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, необходимая работодателю в связи с трудовыми отношениями;

– 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 в порядке, предусмотренном настоящим Федеральным законом;

– обработка персональных данных – сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение персональных данных работников Организации;

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

1.5. К персональным данным работника, получаемым работодателем и подлежащих хранению у работодателя в порядке, предусмотренном действующим законодательством и

настоящим Положением, относятся следующие сведения, содержащиеся в личном деле работников:

- копия паспорта или иной документ, удостоверяющий личность;
- копия страхового свидетельства государственного пенсионного страхования;
- копии документов воинского учета – для военнообязанных и лиц, подлежащих воинскому учету;
- копии документов об образовании, о квалификации или наличии специальных знаний – при поступлении на работу, требующую специальных знаний или специальной подготовки;
- копия свидетельства о присвоении ИНН;
- анкетные данные, заполненные работником при поступлении на работу или в процессе работы (в том числе автобиография, сведения о семейном положении работника, перемене фамилии, наличии детей и иждивенцев);
- документы о возрасте малолетних детей и месте их обучения;
- документы о состоянии здоровья детей и других родственников (включая справки об инвалидности, о наличии хронических заболеваний);
- документы о состоянии здоровья (сведения об инвалидности, о беременности и т.п.);
- иные документы, которые с учетом специфики работы и в соответствии с законодательством Российской Федерации должны быть предоставлены работником при заключении трудового договора или в период его действия (включая медицинские заключения, предъявляемые работником при прохождении обязательных предварительных и периодических медицинских осмотров);
- заключение по данным психологического исследования (если такое имеется);
- иные документы, содержащие сведения о работнике, нахождение которых в личном деле работника необходимо для документального оформления трудовых правоотношений с работником (включая приговоры суда и запрете заниматься педагогической деятельностью или занимать руководящие должности);
- Кадровые документы (трудовой договор, дополнительные соглашения к трудовому договору, приказы, карточка формы Т-2, заявления, объяснительные и служебные записки)

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

- документы, удостоверяющие личность обучающегося (свидетельство о рождении или паспорт);
- документы о месте проживания;
- документы о составе семьи;
- паспортные данные родителей (законных представителей) обучающегося;
- документы о получении образования, необходимые для поступления на обучение по профессии (личное дело, справка с предыдущего места учебы и т.п.);
- полис медицинского страхования;
- документы 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, предоставляющих повышенную опасность для здоровья и т.п.);
- документы, подтверждающие права на дополнительные гарантии и компенсации по определенным основаниям, предусмотренным законодательством (родители-инвалиды, неполная семья, ребенок-сирота и т.п.);

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

II. СОСТАВ И ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ

2.1. В состав персональных данных работников Техникума входят документы, содержащие информацию о паспортных данных, образовании, отношении к воинской обязанности, семейном положении, месте жительства, состоянии здоровья, а также о предыдущих местах их работы.

2.2. Комплекс документов, сопровождающий процесс оформления трудовых отношений работника в Техникуме при его приеме, переводе и увольнении:

2.2.1. Информация, представляемая работником при поступлении на работу в Техникум, должна иметь документальную форму. При заключении трудового договора в соответствии со ст. 65 Трудового кодекса Российской Федерации лицо, поступающее на работу, предъявляет работодателю:

- паспорт или иной документ, удостоверяющий личность;
 - трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства, либо трудовая книжка у работника отсутствует в связи с ее утратой или по другим причинам;
 - страховое свидетельство государственного пенсионного страхования;
 - документы воинского учета – для военнообязанных и лиц, подлежащих воинскому учету;
 - документ об образовании, о квалификации или наличии специальных знаний – при поступлении на работу, требующую специальных знаний или специальной подготовки;
 - свидетельство о присвоении ИНН (при его наличии у работника);
- Работодатель имеет право запрашивать информацию характеризующую деятельность работника с предыдущего места его работы только с согласия субъекта персональных данных.

2.2.2. При оформлении работника в Техникум работником отдела кадров заполняется унифицированная форма Т-2 «Личная карточка работника», в которой отражаются следующие анкетные и биографические данные работника:

- общие сведения (Ф.И.О. работника, дата рождения, место рождения, гражданство, образование, профессия, стаж работы, состояние в браке, паспортные данные);

- сведения о воинском учете;

- данные о приеме на работу;

В дальнейшем в личную карточку вносятся:

- сведения о переводах на другую работу;

- сведения об аттестации;

- сведения о повышении квалификации;

- сведения о профессиональной переподготовке;

- сведения о наградах (поощрениях), почетных званиях;

- сведения об отпусках;

- сведения о социальных гарантиях;

- сведения о месте жительства и контактных телефонах.

2.3. Техникум определяет объем, содержание обрабатываемых персональных данных работников и обучающихся, руководствуясь Конституцией Российской Федерации, Трудовым

кодексом Российской Федерации, Федеральным законом от 29 декабря 2012г. N 273-ФЗ "Об образовании в Российской Федерации" и иными федеральными законами.

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

Обработка персональных данных обучающегося может осуществляться исключительно 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.

2.5. Все 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.

2.6. Персональные данные несовершеннолетнего обучающегося в возрасте старше 14 лет предоставляются самим обучающимся с письменного согласия своих законных представителей - родителей, усыновителей или попечителя. Если персональные данные обучающегося возможно получить только у третьей стороны, то обучающийся должен быть уведомлен об этом заранее. От него и его родителей (законных представителей) должно быть получено письменное согласие на получение персональных данных от третьей стороны. Обучающийся и его родители (законные представители) 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.

2.7. Согласие работника не требуется в следующих случаях:

– обработка персональных данных осуществляется на основании Трудового кодекса РФ или иного федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия работодателя;

– обработка персональных данных осуществляется в целях исполнения трудового договора;

– обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

– обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов работника, если получение его согласия невозможно.

2.8. Техникум не имеет права получать и обрабатывать персональные данные работника и обучающегося о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни. В случаях, непосредственно связанных с вопросами обучения и трудовых отношений, в соответствии со ст. 24 Конституции РФ работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

Обработка указанных персональных данных работников работодателем возможна только с их согласия либо без их согласия в следующих случаях:

- персональные данные являются общедоступными;
- персональные данные относятся к состоянию здоровья работника и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия работника невозможно;
- по требованию полномочных государственных органов в случаях, предусмотренных федеральным законом.

III. ХРАНЕНИЕ И ИСПОЛЬЗОВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Персональные данные работников и обучающихся Техникума хранятся на бумажных и электронных носителях, в специально предназначенных для этого помещениях. Срок хранения документов определяется утвержденной номенклатурой дел. По истечении сроков хранения документы по решению Экспертной комиссии (создается в целях организации и проведения методической и практической работы по экспертизе ценности документов, образовавшихся в деятельности Техникума) подлежат уничтожению в установленном порядке.

3.2. В процессе хранения персональных данных работников и обучающихся Техникума 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 достоверности и полноты персональных данных, их регулярное обновление и внесение по мере необходимости соответствующих изменений.

3.3. Доступ к персональным данным работников и обучающихся образовательного учреждения имеют:

- директор;
- заместители директора;
- главный бухгалтер, бухгалтер;
- руководители структурных подразделений - к персональным данным работников возглавляемых подразделений;
- классные руководители (только к персональным данным обучающихся своей группы);
- мастера производственного обучения (только к персональным данным обучающихся своей группы);
- начальник отдела кадров, инспектор отдела кадров;
- секретарь-машинистка (в филиале Техникума)
- секретарь учебной части (только к персональным данным обучающихся);
- социальный педагог по защите прав детей-сирот и детей, оставшихся без попечения родителей (только к персональным данным детей-сирот и детей, оставшихся без попечения родителей);
- инженер по обслуживанию ЭВТ
- иные работники, определяемые приказом директора Техникума в пределах своей компетенции.

иные работники, определяемые приказом руководителя образовательного учреждения в пределах своей компетенции.

- 3.4. Помимо лиц, указанных в п. 3.3. настоящего Положения, право доступа к персональным данным работников и обучающихся имеют только лица, уполномоченные действующим законодательством.
- 3.5. Лица, имеющие доступ к персональным данным, обязаны использовать персональные данные работников и обучающихся лишь в целях, для которых они были предоставлены.
- 3.6. Ответственным за организацию и осуществление хранения персональных данных работников и обучающихся образовательного учреждения является заместитель директора, в соответствии с приказом директора Техникума.
- 3.7. Персональные данные работника отражаются в личной карточке работника (форма Т-2), которая заполняется после издания приказа о его приеме на работу. Личные карточки работников хранятся в специально оборудованных несгораемых шкафах в алфавитном порядке.
- 3.8. Персональные данные обучающегося отражаются в его личном деле, которое заполняется после издания приказа о его зачислении в образовательное учреждение. Личные дела обучающихся в алфавитном порядке формируются в папках групп, которые хранятся в специально оборудованных несгораемых шкафах.
- 3.9. Запрещается оставлять посторонних лиц в кабинете без присмотра и в отсутствии других работников.
- 3.10. Передача информации, содержащей сведения о персональных данных работников, по телефону в связи с невозможностью идентификации лица, запрашивающего информацию, запрещается.
- 3.11. Обеспечение безопасности персональных данных достигается, в частности:
- определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
 - применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных (п. 3.14. настоящего Положения);
 - применением прошедших в установленном порядке процедур оценки соответствия средств защиты информации;
 - оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
 - учетом машинных носителей персональных данных;
 - обнаружением фактов несанкционированного доступа к персональным данным и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них;
 - восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
 - установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
 - контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

3.12. 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.

3.12.1. 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.

3.12.2. 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.

3.12.3. 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.

3.13. Уровни защищенности персональных данных.

3.13.1. Первый уровень защищенности:

– 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;

– для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100 тысяч субъектов персональных данных, не являющихся сотрудниками Организации.

3.13.2. Второй уровень защищенности.

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

– для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников Организации или специальные категории персональных данных менее чем 100 тысяч субъектов персональных данных, не являющихся сотрудниками Организации;

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

– для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные более чем 100 тысяч субъектов персональных данных, не являющихся сотрудниками Организации;

– для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных более чем 100 тысяч субъектов персональных данных, не являющихся сотрудниками Организации;

– для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100 тысяч субъектов персональных данных, не являющихся сотрудниками Организации.

3.13.3. Третий уровень защищенности.

– для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные сотрудников Организации или

общедоступные персональные данные менее чем 100 тысяч субъектов персональных данных, не являющихся сотрудниками Организации;

- для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных сотрудников Организации или иные категории персональных данных менее чем 100 тысяч субъектов персональных данных, не являющихся сотрудниками Организации;

- для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников Организации или специальные категории персональных данных менее чем 100 тысяч субъектов персональных данных, не являющихся сотрудниками Организации;

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

- для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных более чем 100 тысяч субъектов персональных данных, не являющихся сотрудниками Организации.

3.13.4. Четвертый уровень защищенности.

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

- для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных сотрудников Организации или иные категории персональных данных менее чем 100 тысяч субъектов персональных данных, не являющихся сотрудниками Организации.

3.13.5. При четвертом уровне защищенности персональных данных работодатель:

- обеспечивает режим безопасности помещений, в которых размещаете информационную систему;

- обеспечивает сохранность носителей информации;

- утверждает распорядительным актом перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

- использует средства защиты информации, которые прошли процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

3.13.6. При третьем уровне защищенности персональных данных дополнительно к мерам, перечисленным в пункте 3.13.3. настоящего Положения, работодатель назначает ответственного за обеспечение безопасности персональных данных в информационной системе.

3.13.7. При втором уровне защищенности персональных данных дополнительно к мерам, перечисленным в пункте 3.13.2. настоящего Положения, работодатель ограничивает доступ к электронному журналу сообщений, за исключением работников, которым такие сведения необходимы для работы.

3.13.8. При первом уровне защищенности персональных данных дополнительно к мерам, перечисленным в пункте 3.13.1. настоящего Положения, работодатель:

- обеспечивает автоматическую регистрацию в электронном журнале безопасности изменения полномочий работников по допуску к персональным данным в системе;

- создает отдел, ответственный за безопасность персональных данных в системе, либо возлагает такую обязанность на один из существующих отделов работодателя.

- 3.14. В целях защиты персональных данных на бумажных носителях работодатель:
- приказом назначает ответственного за обработку персональных данных;
 - ограничивает допуск в помещения, где хранятся документы, которые содержат персональные данные работников;
 - хранит документы, содержащие персональные данные работников в шкафах, запирающихся на ключ;
 - хранит трудовые книжки работников в сейфе в отделе кадров.

IV. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. При передаче персональных данных работников и обучающихся образовательного учреждения другим юридическим и физическим лицам образовательное учреждение должно соблюдать следующие требования:

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

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

4.2. 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.

V. ПРАВА РАБОТНИКОВ, ОБУЧАЮЩИХСЯ НА ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. В целях обеспечения защиты персональных данных, хранящихся у образовательного учреждения, работники, обучающиеся (родители (законные представители) малолетнего несовершеннолетнего обучающегося), имеют право:

5.1.1. получать полную информацию о своих персональных данных и их обработке;

5.1.2. 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, обучающегося (для несовершеннолетнего - его родителей, законных представителей) — к заместителю директора, ответственному за организацию и осуществление хранения персональных данных работников;

5.1.3. требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением требований действующего законодательства. Указанное требование должно быть оформлено письменным заявлением работника на имя руководителя образовательного учреждения.

При отказе руководителя образовательного учреждения исключить или исправить персональные данные работника работник, обучающийся (родитель, законный представитель

несовершеннолетнего обучающегося) имеет право заявить в письменном виде руководителю образовательного учреждения о своем несогласии, с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник, обучающийся (родитель, законный представитель несовершеннолетнего обучающегося) имеет право дополнить заявлением, выражающим его собственную точку зрения;

5.1.4. требовать извещения образовательным учреждением всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обучающегося (воспитанника) обо всех произведенных в них исключениях, исправлениях или дополнениях;

5.1.5. обжаловать в суде любые неправомерные действия или бездействия образовательного учреждения при обработке и защите его персональных данных.

VI. ОБЯЗАННОСТИ СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ ПО ОБЕСПЕЧЕНИЮ ДОСТОВЕРНОСТИ ЕГО ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. В целях обеспечения достоверности персональных данных работники обязаны:

6.1.1. при приеме на работу в образовательное учреждение представлять уполномоченным работникам образовательного учреждения достоверные сведения о себе в порядке и объеме, предусмотренном законодательством Российской Федерации;

6.1.2. 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 в течение 5 рабочих дней со дня их изменений.

6.2. В целях обеспечения достоверности персональных данных обучающиеся (родители, законные представители несовершеннолетних обучающихся) обязаны:

6.2.1. при приеме в образовательное учреждение представлять уполномоченным работникам образовательного учреждения достоверные сведения о себе (своих несовершеннолетних детей);

6.2.2. в случае изменения сведений, составляющих персональные данные несовершеннолетнего обучающегося старше 14 лет, он обязан в течение 10 дней сообщить об этом уполномоченному работнику образовательного учреждения.

VII. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НАСТОЯЩЕГО ПОЛОЖЕНИЯ

7.1. За нарушение порядка обработки (сбора, хранения, использования, распространения и защиты) персональных данных должностное лицо несет административную ответственность в соответствии с действующим законодательством.

7.2. За нарушение правил хранения и использования персональных данных, повлекшее за собой материальный ущерб работодателю, работник несет материальную ответственность в соответствии с действующим трудовым законодательством.

7.3. Материальный ущерб, нанесенный субъекту персональных данных за счет ненадлежащего хранения и использования персональных данных, подлежит возмещению в порядке, установленном действующим законодательством.

7.4. Техникум вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных лишь обработку следующих персональных данных:

- относящихся к субъектам персональных данных, которых связывают с оператором трудовые отношения (работникам);
- полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных (обучающийся и др.), если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;
- являющихся общедоступными персональными данными;
- включающих в себя только фамилии, имена и отчества субъектов персональных данных;
- необходимых в целях однократного пропуска субъекта персональных данных на территорию образовательного учреждения или в иных аналогичных целях;
- включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус федеральных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка (включая базы данных, формируемые в связи с ЕГЭ);
- обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных.

Во всех остальных случаях оператор (руководитель образовательного учреждения и (или) уполномоченные им лица) обязан направить в уполномоченный орган по защите прав субъектов персональных данных соответствующее уведомление.

VIII. ГАРАНТИИ КОНФИДЕНЦИАЛЬНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Все работники организации, осуществляющие обработку персональных данных, обязаны хранить тайну о сведениях, содержащих персональные данные, в соответствии с настоящим Положением, требованиями законодательства Российской Федерации.

8.2. Работник вправе требовать полную информацию о своих персональных данных, об их обработке, использовании и хранении.

8.3. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работников, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством.