Департамент образования и науки Кемеровской области
Государственное профессиональное образовательное учреждение
«Киселевский горный техникум»
(ГПОУ КГТ)

УТВЕРЖДАЮ
Директор ГПОУ КГТ
_____ Л.А. Чеснокова
«12» января 2016 г.

ПОЛОЖЕНИЕ

об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных ГПОУ КГТ

Киселёвск 2016

1. **Общие положения**

1.1.Положение об обеспечении безопасности персональных данных при обработке их в информационной системе персональных данных (далее – Положение) в Государственном профессиональном образовательном учреждении «Киселевский горный техникум» (далее Оператор) разработано в соответствии:

- с частью 1 статьи 23, статьи 24 Конституции Российской Федерации,
-Указом Президента Российской Федерации от 06 марта 1997 № 188 «Об утверждении перечня сведений конфиденциального характера»;
главой 14 Трудового кодекса Российской Федерации (далее ТК РФ),
-Гражданским кодексом Российской Федерации,
-Федеральным законом от 27 июля 2006г. N 152-ФЗ «О персональных данных»,
-Федеральным законом от 27 июля 2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»,
-Федеральным законом от 19 декабря 2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»,
- Федеральным законом от 29 декабря 2012 года № 273-ФЗ «Об образовании в Российской Федерации»;
-Федеральным законом от 02.05.2006 №59-ФЗ "О порядке рассмотрения обращений граждан Российской Федерации",
-Постановлением Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»,
-Постановлением Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»,
-Постановлением Правительства РФ от 10 июля 2013 г. N 582 "Об утверждении Правил размещения на официальном сайте образовательной организации»,
-Постановлением Правительства Российской Федерации от 15 августа 2013 г. № 706 «Об утверждении Правил оказания платных образовательных услуг»; -Приказом ФСТЭК от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
-Лицензией на право ведения образовательной деятельности, регистрационный №15679 от 20.01.2016 г.
-Уставом ГПОУ КГТ, утвержденным от 23.12.2015 г.

1.2.Настоящее Положение определяет порядок обработки персональных данных работников техникума, обеспечения безопасности при обработке персональных данных, а также установления ответственности должностных лиц, за невыполнение требований, регулирующих обработку и защиту персональных

данных.

1.3.Целями настоящего Положения являются:

- обеспечение соответствия действий Оператора при обработке персональных данных работников техникума требованиям законодательства Российской Федерации, обеспечения защиты их прав и свобод при обработке их персональных данных, обеспечение защиты персональных данных от несанкционированного доступа, утраты, неправомерного их использования или распространения.

1.4. Требования настоящего Положения являются обязательными для исполнения всеми сотрудниками Оператора, получившими доступ к персональным данным.

1.5. Настоящее Положение вступает в силу с момента утверждения директором техникума и действует бессрочно, до замены его новым нормативным документом. Все изменения в Положение вносятся приказом директора.

1.6.Работники техникума должны быть ознакомлены с настоящим Положением под подпись.

1.7.В настоящем Положении используются следующие понятия и термины:

– **персональные данные (ПДн)** – любая информация, относящаяся к прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных);

-субъект персональных данных– лица, носители персональных данных, передавшие свои персональные данные как на добровольной основе, так и в рамках выполнения требований нормативно-правовых актов для обработки персональных данных;

– **оператор** – юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

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

-конфиденциальность персональных данных - обязательное для соблюдения должностным лицом техникума, иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;

-автоматизированная обработка персональных данных–обработка персональных данных с помощью средств вычислительной техники;

-распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

-использование персональных данных- действия (операции) с персональными данными, совершаемые должностным лицом Техникума в целях принятия решений или совершения иных действий, порождающих юридические последствия в

отношении субъектов персональных данных либо иным образом затрагивающих их права и свободы или права и свободы других 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;
-общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;
-информация - сведения (сообщения, данные) независимо от формы их представления;
-информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
-трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;
–**защита персональных данных** – жестко регламентированный технологический процесс,предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных, обеспечивающий надежную безопасность информации в процессе деятельности Техникума.
-актуальные угрозы безопасности персональных данных- совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатомкоторого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

2. Понятие и состав персональных данных

2.1. Персональные данные работника – информация, необходимая работодателю в связи с трудовыми отношениями и касающиеся конкретного работника. Под информацией о работниках понимаются сведения о фактах, событиях и обстоятельствах жизни работника, позволяющие идентифицировать его личность.

2.2.В состав персональных данных работников входят:

–анкетные и биографические данные (фамилия, имя, отчество; год, месяц, дата и место рождения;
-паспортные данные (серия, номер документа, дата выдачи, наименование органа, выдавшего документ, гражданство, а также иные данные, содержащиеся в удостоверении личности работника);
–сведения об образовании работника (полученной специальности, квалификации, сведения документов об образовании, наличии специальных знаний или подготовки;
–сведения о трудовом и общем, педагогическом стаже;
–сведения о семейном положении, о составе семьи, фамилии, имена, отчества, даты рождения членов семьи;
-сведения об отношении к воинской обязанности, сведения военного билета, иных документов воинского учета;
–сведения о доходах, включая размер должностного оклада, надбавок, доплат и других выплат;
-сведения о социальных льготах;
-номер лицевого счета в банке, номер карты;
–сведения о профессии, специальности работника, занимаемой должности;
- сведения о наличии/отсутствии судимости;
–адрес места жительства;
–контактный телефон;
-данные об изображении лица;
–содержание трудового договора;
–подлинники и копии приказов по личному составу;
–личные дела, личные карточки (форма Т-2) и трудовые книжки сотрудников;
–основания к приказам по личному составу;
–дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
–автобиография;
–данные, содержащиеся в трудовой книжке работника, страховом свидетельстве государственного пенсионного страхования, свидетельстве о постановке на налоговый учет;
–данные, содержащиеся в документах воинского учета (при их наличии);
–документы о состоянии здоровья работника (с целью возможности выполнения трудовой функции-медицинские книжки, сертификаты о прививках, листки нетрудоспособности);
-сведения о наличии инвалидности, программа реабилитации;
Перечень персональных данных, обрабатываемых Оператором определен в Приложении 1.

3.Обработка персональных данных

3.1.Получение персональных данных:
3.1.1.При заключении трудового договора лицо, поступающее на работу,

предоставляет достоверные сведения о себе в документированной форме:
-заявление;
-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 (в ней содержатся сведения о трудовом стаже, предыдущих местах работы);
-страховое свидетельство государственного пенсионного страхования (для уплаты за работника соответствующих взносов);
-документы воинского учета - для лиц, подлежащих воинскому учету (для осуществления в техникуме воинского учета);
-документ об образовании, о квалификации и наличии специальных знаний - при поступлении на работу, требующую специальных знаний или специальной подготовки (подтверждают квалификацию работника, обосновывают занятие определенной должности); водительское удостоверение (для оформления на должность водителя);
-справку о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям (требования ст.331, 351.1. ТК РФ).

Запрещается требовать от лица, поступающего на работу, документы помимо предусмотренных Трудовым кодексом РФ, иными федеральными законами.

3.1.2.В ходе трудовой деятельности может возникнуть необходимость в предоставлении Работником иных документов:
-свидетельство о заключении брака, о составе семьи, о рождении детей, о беременности женщины, об инвалидности, о донорстве, о доходах с предыдущего места работы, о необходимости ухода за больным членом семьи, индивидуальный номер налогоплательщика, свидетельство о смерти, свидетельство о рождении детей, прочие документы, которые могут понадобиться Оператору для предоставления работнику определенных льгот, социальных гарантий, предусмотренных законодательством.

3.1.3.Работодатель вправе проверять достоверность сведений, предоставляемых Работником. Предоставление работником подложных документов или ложных сведений при поступлении на работу является основанием для расторжения трудового договора.

3.1.4.Работником отдела кадров заполняется унифицированная форма Т-2- «Личная карточка работника», в которой отражаются анкетные и биографические данные работника:

-общие сведения (Ф.И.О. работника, пол, дата рождения, месторождения, гражданство, образование, профессия, специальность, стаж работы, состояние в браке, состав семьи, паспортные данные);
-сведения о месте жительства и о контактных телефонах;
-номер страхового свидетельства государственного пенсионного страхования;
-идентификационный номер налогоплательщика;
-сведения о воинском учете;

-данные о приеме на работу (табельный номер, должность, структурное подразделение, размер оклада, номер и дата приказа, номер трудового договора, дата заключения трудового договора, вид договора, характер работы);
-сведения о социальных гарантиях.

3.1.5. 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 использовании отпусков;
-сведения об увольнении.

Все вышеуказанные персональные данные вносятся в информационную программу «1С: Предприятие».

3.1.6. Все предоставленные документы хранятся в личном деле. Личное дело ведется на протяжении всей трудовой деятельности работника. Изменения, вносимые в личное дело, должны быть подтверждены соответствующими документами.

3.1.7.Документы, содержащие персональные данные работников, являются конфиденциальными. Лица, получающие персональные данные Работника обязаны соблюдать режим секретности (конфиденциальности). Учитывая массовость и единое место обработки и хранения конфиденциальных документов, содержащих персональные данные, гриф ограничения на них не ставится. Режим конфиденциальности в отношении персональных данных снимается в случае:
обезличивания персональных данных, по истечении 75 лет срока их хранения и для общедоступных персональных данных, т.е. включенных в справочники, адресные книги и т.п.

3.1.8.Все персональные данные Оператор получает непосредственно от работника. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Оператор 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.

3.1.9.Не допускается обработка специальных категорий персональных данных о расовой, национальной принадлежности, политических, религиозных или философских убеждениях, частной жизни, о членстве в общественных объединениях или профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.
Оператор не получает и не обрабатывает сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные).

3.1.10.Оператор не вправе обрабатывать информацию о состоянии здоровья субъекта персональных данных за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции, а также

случаев, когда их обработка необходима для защиты жизни, здоровья или иных жизненно важных интересов субъектов персональных данных либо других лиц.

3.1.11.Общим условием обработки персональных данных работников является наличие письменного согласия субъекта персональных данных на осуществление такой обработки. Согласие работника должно быть добровольным, конкретным и информированным. Форма согласия утверждается приказом директора (Приложение №2).

3.1.12. 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;

-при поступлении официальных запросов из надзорно-контрольных или правоохранительных органов (суд, прокуратура. ФСБ, МВД и т.п.) или при непосредственном обращении сотрудников вышеуказанных органов, при предъявлении ими служебных удостоверений и соответствующих документов о получении персональных данных, а также в случаях, предусмотренных федеральным законом;

- обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных;

- 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;

- обработка персональных данных осуществляется при регистрации и отправке корреспонденции почтовой связью;

-обработка персональных данных осуществляется в целях профессиональной деятельности журналиста либо в целях научной, литературной или иной творческой деятельности, при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

-обработка персональных данных осуществляется при оформлении разовых пропусков в техникум.

3.1.13. Получать согласие на обработку персональных данных нужно также:

-от соискателя на замещение вакантной должности на период принятия работодателем решения о приеме либо отказе в приеме на работу, (Приложение №8). Не требуется согласие на обработку персональных данных от соискателя при получении их от кадрового агентства, действующего от имени соискателя, с которым он заключил договор, либо соискатель сам разместил свое резюме в Интернете, сделав его доступным неограниченному кругу лиц.

3.1.14.Работник в любое время вправе отозвать согласие на обработку персональных данных.

4. Способы обработки персональных данных

4.1 Документы, содержащие персональные данные создаются путем:

-получения оригиналов необходимых документов (трудовая книжка, автобиография, личный листок по учету кадров);
-копирования, сканирования оригиналов (документ об образовании);
-внесения сведений в учетные формы (на бумажных и электронных носителях).

4.2.Информация о персональных данных может содержаться на бумажных и электронных носителях, в автоматизированных информационных системах.

4.3.Обработка персональных данных может производиться как с использованием средств автоматизации, так и без использования таких средств, т.е. смешанным способом.

4.4.Обработка персональных данных, содержащихся в информационной системе персональных данных, либо извлеченных из такой системы, считается осуществленной 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. (Постановления Правительства - от 15.09.2008 N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации" (далее - Постановление N 687) и от 17.11.2007 N 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных").

4.5.Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на разных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков).

4.6.Не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо несовместимы.

4.7.При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее-типовая форма), должны соблюдаться следующие условия:
-типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, наименование Оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источники получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых способов обработки персональных данных;
-типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации – при необходимости получения письменного согласия на обработку персональных данных;
-типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

4.8.При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

-при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию и используется (распространяется) копия персональных данных;

-при необходимости уничтожения части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных, зафиксированных на материальном носителе (удаление, вымарывание).

4.9.Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя- путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем изготовления нового материального носителя с уточненными персональными данными.

4.10.Обработка персональных данных с использованием средств автоматизации может производиться только с применением учтенных технических средств и носителей информации, имеющих необходимый для каждой категории персональных данных, технический и программный уровень защиты.

4.11.Для каждого пользователя автоматизированных систем персональных данных создается индивидуальный уникальный пароль доступа в информационную систему персональных данных.

4.12.При обработке персональных данных с применением объектов вычислительной техники должностные лица, осуществляющие такую обработку, должны быть ознакомлены под подпись с локальными нормативными актами Оператора, устанавливающими порядок применения объектов вычислительной техники.

5. Доступ к персональным данным

5.1.Доступ к персональным данным, обрабатываемым в ГПОУ КГТ, разрешается только специально уполномоченным лицам, и только к тем персональным данным, которые необходимы для выполнения конкретных функций.

5.2.Внутренний доступ к персональным данным субъектов персональных данных имеют:

-директор,

-заместители директора,

-руководители структурных подразделений (персональные данные подчиненного

им работника),

-председатель выборного органа первичной профсоюзной организации техникума,

-работники, специально уполномоченные на обработку персональных данных (доступ только к тем персональным данным, которые необходимы для выполнения конкретных функций);

-субъект персональных данных.

5.3.Доступ к персональным данным может быть предоставлен иному сотруднику Работодателя, должность которого не поименована в списке лиц, имеющих доступ к персональным данным работника, если этого требует производственная необходимость и выполняемая им трудовая функция. Для этого сотруднику следует составить докладную записку на имя директора с визой непосредственного руководителя.

5.4.Перечень должностей сотрудников, имеющих доступ к персональным данным работников утверждается приказом директора (Приложение №3).

5.5.Перечень лиц, осуществляющих обработку персональных данных работников в информационной системе определяется приказом директора техникума (Приложение №4).

5.6.Должностные лица, имеющие доступ к персональным данным в силу исполнения ими своих должностных обязанностей, при их обработке обязаны:

- знать и выполнять требования законодательства в области обеспечения защиты персональных данных, настоящего Положения;
- обеспечивать конфиденциальность этих сведений, не раскрывать третьим лицам и не распространять персональные данные, ставшие известные ему в связи с выполнением трудовой функции, без согласия субъекта персональных данных, если иное не предусмотрено Федеральным законом;

-подписать Обязательство о неразглашении конфиденциальной информации (Приложение № 5);

-информировать директора техникума о фактах нарушения порядка обращения с персональными данными, о попытках несанкционированного доступа к ним;

-соблюдать правила использования персональных данных, порядок их учета и хранения, исключить доступ к ним посторонних лиц;

-обрабатывать только те персональные данные, к которым получен доступ в силу исполнения трудовых обязанностей;

запрещается:

- использовать сведения, содержащие персональные данные, в неслужебных целях, а также в служебных целях – при ведении переговоров по телефонной сети, в открытой переписке, статьях и выступлениях;

-передавать персональные данные по незащищенным каналам связи (факсимильная связь, электронная почта и т.д.) без использования сертифицированных антивирусных средств;

-снимать копии с документов и других носителей информации, содержащих персональные данные, или производить выписки из них, а равно использовать различные технические средства для фиксации сведений, содержащих персональные данные, без разрешения директора учреждения; - выполнять на дому работы, связанные с использованием персональных данных, выносить документы и другие

носители информации, содержащие персональные данные, из здания учреждения без разрешения директора учреждения.

5.7.Обеспечение конфиденциальности персональных данных не требуется в случае обезличивания персональных данных, для общедоступных персональных данных (включенных в справочники, адресные книги и т.п.).

5.8.Внешний доступ (другие организации и граждане)

5.8.1.К числу внешних потребителей персональных данных можно отнести государственные и негосударственные структуры: налоговые органы, пенсионные фонды, органы социального страхования, обязательного медицинского страхования, военкоматы, органы статистики, подразделения государственных и муниципальных органов управления, органы прокуратуры, судебные, правоохранительные органы, органы службы безопасности, лицензирующие и надзорно-контрольные органы, вышестоящая организация, иные органы и организации, граждане).

5.8.2.Внешний доступ к персональным данным разрешается только при наличии заявления запросившего лица с указанием перечня необходимой информации, целей, для которых она будет использована с письменного согласия субъекта персональных данных.

6.Хранение и использование персональных данных работников:

6.1.В отделе кадров техникума создаются и хранятся следующие группы документов, содержащие персональные данные работников в единичном или сводном виде :

6.1.1. комплекс документов, сопровождающий процесс оформления трудовых отношений при приеме на работу, переводе, увольнении:

-личные дела работников (автобиография, личный листок, дополнение к личному листку, заявления, трудовые договоры, дополнительные соглашения к трудовым договорам, соглашения сторон, уведомления, согласия работниковна обработку персональных данных, копии документов об образовании и наличии специальных знаний, аттестационные листы, копии свидетельств, удостоверений о повышении квалификации, профессиональной переподготовке, фотография, согласие);

-личные карточки ф.Т-2;

-трудовые книжки работников, вкладыши в трудовую книжку;

-медицинские книжки;

-подлинники и копии приказов по личному составу (о приеме на работу, об увольнении, о переводе, о предоставлении отпуска, о направлении в командировку, о поощрении, о взыскании, о внесении изменений в учетные данные, о предоставлении отпуска по уходу за ребенком);

-приказы об изменении условий трудового договора, о совмещении, о премировании, о доплатах, о выплатах социального характера, о выплате пособий в связи с рождением ребенка, о выплатах при сокращении, о материальной помощи)

-приказы по обучению, по аттестации, о присвоении категории, основания к приказам;

-журнал регистрации движения трудовых книжек и вкладышей в них;

-журналы регистрации приказов,

-журнал регистрации командировок,

-журналы регистрации выдачи справок работникам,
-журналы регистрации обращений граждан;
-журнал регистрации листков нетрудоспособности;
-журнал регистрации приемов и увольнений работников;
-журнал регистрации личных дел, карточек ф.Т-2;
-объяснительные, акты, протоколы;
-график отпусков;
-табели учета использования рабочего времени;
-штатное расписание (копии);
-должностные инструкции работников;
справочно-информационный банк данных по персоналу(списки, картотеки, журналы регистрации);
-материалы служебных расследований (объяснительные записки, акты, приказы);
-журнал ознакомления работников с локальными актами в области обработки и защиты персональных данных;

6.1.2.документы по собеседованию с кандидатом на вакантную должность (копии документов об образовании, наличии специальных знаний, сведения о повышении квалификации, профессиональной переподготовке, согласие на обработку персональных данных);

6.1.3.организационно-распорядительные документы (приказы, распоряжения, указания руководства техникума);

6.1.4.документы по организации работы структурных подразделений(положения, документы по планированию, учету, анализу и отчетности, копии отчетных, аналитических и справочных материалов).

6.2. В бухгалтерии создаются и/или хранятся следующие группы документов, содержащих персональные данные работников:
-доверенности на работников;
-договоры, связанные с осуществлением деятельности Оператора;
-расчетные листки работников;
-ведомости с номерами расчетных счетов работников;
-документы, необходимые для расчета заработной платы работников, которые передаются в бухгалтерию сотрудником отдела кадров;
-листки нетрудоспособности;
-заявления работников на удержания, на открытие банковской карты, на выплаты, компенсаций, материальной помощи, пособий;
-подтверждающие документы для предоставления социальных гарантий;
-исполнительные листы.

6.3. В отделе информационных технологий хранятся:
-заявления на открытие(блокирование, уничтожение) учетной записи,
-акты приема/передачи оборудования,
-журнал регистрации электронных носителей,
-журнал регистрации паролей доступа,
-заявления на изготовление пропусков работников,

6.4.Хранение персональных данных должно осуществляться в соответствии с требованиями законодательства, устанавливающие правила хранения

конфиденциальных сведений, сохранность имеющихся данных, ограничение доступа к ним, исключающем их утрату или их неправомерное использование.
6.5.Все материальные носители персональных данных подлежат учету.
6.6.Необходимо обеспечивать раздельное хранение персональных данных на разных материальных носителях, обработка которых осуществляется в различных целях.
6.7.Хранение персональных данных (документов, материальных носителей персональных данных и др.) допускается только в помещениях, оборудованных надежными замками, в запирающихся шкафах и сейфах, исключающих возможность доступа третьих лиц (Приложение №6).
6.8.В электронном виде персональные данные хранятся в автоматизированной информационной системе «1С: Предприятие» (базы данных по учету работников, базы данных бухгалтерии), региональной автоматизированной информационной системе «Электронное профессиональное образование» (АИС-ЭПО), доступ к которым ограничивается системой паролей. В локальной сети Оператора допускается хранение только общедоступных персональных данных. На официальном сайте Оператора допускается размещение только общедоступных персональных данных. Размещение иных персональных данных (в т.ч. фотографических изображений) субъекта персональных данных осуществляется с письменного согласия субъекта персональных данных.
6.9.Обязанности по хранению личных дел работников, заполнению и выдаче трудовых книжек (дубликатов трудовых книжек), иных документов, отражающих персональные данные работников, возлагаются на специалиста по кадрам и закрепляются в должностной инструкции.
6.10.Оператор осуществляет хранение персональных данных в форме, позволяющей определить субъекта персональных данных не дольше, чем этого требуют цели обработки.
6.11.Контроль за хранением и использованием материальных носителей персональных данных, находящихся на этих носителях, осуществляют руководители структурных подразделений.

7.Уточнение, блокирование и уничтожение персональных данных

7.1.Уточнение персональных данных, в том числе их обновление и изменение, имеет своей целью обеспечение достоверности, полноты и актуальности персональных данных, обрабатываемом Оператором.
7.2.Уточнение персональных данных осуществляется оператором по собственной инициативе, по требованию субъекта персональных данных или его законного представителя, по требованию уполномоченного органа по защите прав субъектов персональных данных в случае, когда установлено, что персональные данные являются неполными, устаревшими, недостоверными.
7.3.Блокирование персональных данных осуществляется Оператором по требованию субъекта персональных данных или его законного представителя, а также по требованию уполномоченного органа по защите прав субъектов персональных данных в случае выявления недостоверных персональных данных или неправомерных действий с ними.

7.4.Об уточнении, блокировании, уничтожении персональных данных Оператор обязан уведомить субъекта персональных данных или его законного представителя.

7.5.Уничтожение персональных данных производится в случаях, предусмотренных законодательством Российской Федерации;

-по достижении цели обработки персональных данных;

-в случае утраты необходимости в достижении целей обработки персональных данных;

-по требованию субъекта персональных данных или уполномоченного органа по защите прав субъектов персональных данных в случае совершения оператором неправомерных действий с персональными данными, когда устранить соответствующие нарушения не представляется возможным.

7.6.Вопрос об уничтожении выделенных документов, содержащих персональные данные, рассматривается на заседании Комиссии по вопросам обработки и защиты персональных данных Оператора. По итогам заседания составляется протокол и акт о выделении к уничтожению документов (Приложение №7) с указанием уничтожаемых дел. Акт утверждается директором ГПОУ КГТ.

7.7.Уничтожение персональных данных на электронных носителях производится путем механического нарушения целостности носителя, не позволяющего произвести их восстановление или методом удаления остаточной информации.

7.8.При уничтожении персональных данных (на бумажном и (или) электронном носителях) Комиссией по вопросам обработки и защиты персональных данных составляется акт согласно установленной формы (Приложение №-8).

8.Сроки обработки персональных данных

8.1.Срок обработки персональных данных определяется периодом времени, в течение которого Оператор осуществляет действия (операции) в отношении персональных данных, обусловленные заявленными целями их обработки, в т.ч. хранение персональных данных.

8.2.Обработка персональных данных начинается с момента их получения оператором и заканчивается:

-по достижении заранее заявленных целей обработки;

-по факту утраты необходимости в достижении заранее заявленных целей обработки;

-в связи с отзывом согласия на обработку персональных данных субъекта персональных данных;

-в связи с ликвидацией юридического лица.

8.3.Сроки хранения персональных данных работников на бумажных носителях устанавливаются в соответствии с Перечнем типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организацией, с указанием сроков хранения, утвержденным приказом Минкультуры России от 25.08.2010 №558 и номенклатурой дел учреждения.

8.4. Персональные данные, содержащиеся в приказах (распоряжениях) по личному составу, в личных делах сотрудников, подлежат хранению в кадровом подразделении в течение пяти лет, с последующей передачей указанных документов

в архив техникума в порядке, предусмотренном законодательством Российской Федерации, где хранятся в течение 75 лет.

8.5. Персональные данные, содержащиеся в приказах о предоставлении отпусков, о краткосрочных командировках, о дисциплинарных взысканиях сотрудников, подлежат хранению в кадровом подразделении в течение пяти лет с последующим их уничтожением.

8.6. Персональные данные, содержащиеся в документах претендентов на замещение вакантной должности техникума, хранятся в кадровом подразделении до замещения вакансии, после чего подлежат уничтожению.

8.7. Бухгалтерские документы, содержащие персональные данные о заработной плате работников, хранятся в течение пяти лет в кабинете бухгалтерии с последующей передачей их на хранение в архив техникума, где хранятся 75 лет.

8.8. Сроки хранения персональных данных работников на электронных носителях: не дольше, чем этого требуют цели обработки.

9. Передача персональных данных

9.1. Передача персональных данных работников производится Оператором только при соблюдении следующих требований:

9.1.1 в целях исполнения Оператором требований действующего законодательства РФ;

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

9.1.3.-не сообщать персональные данные работника в коммерческих целях без его письменного согласия. Обработка персональных данных работников в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только с его предварительного согласия.

9.1.4.-предупредить лиц, получивших персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получившие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное Положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами.

9.1.5.-осуществлять передачу персональных данных работников в пределах техникума в соответствии с настоящим Положением.

9.1.6.-разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретной функции.

9.1.7.-передавать персональные данные работника представителям работников в порядке, установленном Трудовым кодексом Российской Федерации, и

ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функции.

9.2.В рамках Техникума специалист отдела кадров передает в бухгалтерию ведущему бухгалтеру для начисления заработной платы работникам копии приказов, соглашений, листки нетрудоспособности, табели учета использования рабочего времени, справки, свидетельства, заявления, и другие необходимые копии и оригиналы документов.

9.3.Передача документов (иных материальных носителей), содержащих персональные данные работников, осуществляется при наличии у лица, уполномоченного на их получение:

– письма-запроса от третьего лица на бланке организации, которое должно включать всебя указание на основания получения доступа к запрашиваемой информации, содержащей персональные данные работника, её перечень, цель использования, Ф.И.О. и должность лица, которому поручается получить данную информацию с приложением согласия субъекта персональных данных на предоставление персональных данных.

9.4.Согласие работника не требуется, если обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, а также в соответствии с уголовно-исполнительным законодательством Российской Федерации.

9.5.Оператор вправе поручить обработку персональных данных другом лицу с согласия субъекта персональных данных, если иное не предусмотрено Федеральным законом, на основании заключаемого с этим лицом договора, в котором определяется перечень передаваемых персональных данных, перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, цели обработки, устанавливается обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также указываются требования к защите обрабатываемых персональных данных. Лицо, осуществляющее обработку персональных данных по поручению Оператора, несет ответственность перед Оператором и подписывает Соглашение о неразглашении конфиденциальной информации.

10. Мероприятия по обеспечению безопасности персональных данных

Оператором применяются правовые, организационные и технические меры по обеспечению безопасности персональных данных при их обработке в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных».

10.1. Защита персональных данных от неправомерного их использования или утраты обеспечивается Оператором за счет собственных средств.

10.2. Защите подлежат:

-информация о персональных данных субъектов персональных данных, содержащаяся в информационных системах;

-документы, содержащие персональные данные субъектов персональных данных;

-носители персональных данных (бумажные, электронные);

-технические средства (в том числе средства вычислительной техники, машинные носители информации, средства и системы связи и передачи данных, технические средства видеоинформации);
-общесистемное, специальное программное обеспечение, а также средства защиты информации.

10.3.Для обеспечения внутренней защиты персональных данных работников:
-приказом директора назначается ответственный организацию обработки персональных данных и ответственный за обеспечение информационной безопасности в техникуме.
-организуется работа Комиссии по вопросам обработки и защиты персональных данных. Состав комиссии утверждается приказом директора техникума.
-разрабатываются и утверждаются локальные нормативные правовые акты по вопросам обработки и защиты персональных данных субъектов персональных данных;
-утверждается план мероприятий по защите персональных данных, план внутреннего контроля проводимых мероприятий;
-создаются условия, обеспечивающие сохранность персональных данных.
-назначаются работники, уполномоченные на обработку персональных данных:
-определяется состав и категории обрабатываемых в ГПОУ КГТ персональных данных;
-утверждается перечень должностей, имеющих доступ к персональным данным в связи с выполнением трудовой функции, перечень лиц, осуществляющих обработку персональных данных;
-утверждается порядок допуска работников ГПОУ КГТ к обработке персональных данных,
-утверждается порядок доступа работников ГПОУ КГТ в помещения, в которых обрабатываются персональные данные;
-утверждается порядок удаления персональных данных;
-утверждается список мест хранения материальных носителей персональных данных;
-утверждается план размещения автоматизированных рабочих мест;
-утверждается порядок выявления инцидентов информационной безопасности в информационной системе.

10.4. Кадровая служба обеспечивает:
-ознакомление сотрудников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, с настоящим Положением и иными нормативными актами Оператора (приказами, распоряжениями, инструкциями и т.п.), регулирующими обработку и защиту персональных данных работника с данными актами, под подпись.

10.5.Сотрудники, осуществляющие обработку персональных данных, подписывают письменное обязательств о соблюдении конфиденциальности и соблюдении правил обработки персональных данных.

10.6.Производится персональный инструктаж работников по обеспечению конфиденциальности при обращении с информацией, содержащей персональные

данные, предупреждению их об ответственности за нарушение порядка обработки и защиты персональных данных, разглашение и утрату.

10.7. Осуществляется внутренний контроль соответствия обработки персональных данных требованиям законодательства в области защиты персональных данных и принятыми локальными актами Оператора в соответствии с требованиями Постановления Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

10.8 На основе модели угроз разрабатывается система защиты персональных данных, обеспечивающих нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

10.9.Ведется учет применяемых средств защиты информации, носителей персональных данных;

10.10.Устанавливаются индивидуальные пароли доступа сотрудников в информационную систему в соответствии с должностными обязанностями;

10.11.Выявляются факты несанкционированного доступа к персональным данным и принятием соответствующих мер по восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

10.12. Ведется учет обращений субъектов персональных данных;

10.13.Администратор безопасности информационных систем обеспечивает организацию и контроль защиты персональных данных при обработке их в информационных системах персональных данных:

-защита сведений, хранящихся в электронных базах данных, от несанкционированного доступа, искажения и уничтожения информации, а также от иных неправомерных действий, обеспечивается разграничением прав доступа с использованием учетных записей и системы паролей;

-защита обмена персональными данными при их обработке в информационных системах обеспечивается реализацией соответствующих организационных мер;

-размещение информационных систем, специального оборудования и охрану помещений, в которых находятся сервера с базами данных, содержащих персональную информацию;

-контроль за предотвращением воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

-организация возможности восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

-организация обучения лиц, использующих средства защиты информации, применяемых в информационных системах, правилам работы с ними;

-обеспечение учета применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

-контроль соблюдения условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

-организация разбирательств и составление заключений по фактам несоблюдения

условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

10.14.Администратор безопасности информационных систем инициирует организационные, технические и программные мероприятия по обеспечению безопасности персональных данных в информационных системах:

-определению возможных угроз безопасности персональных данных при их обработке в информационных системах, формированию модели угроз, определению класса информационной системы;

-разработке на основе модели угроз системы защиты информационных систем, содержащих персональные данные;

-обеспечение установки и ввода в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

-проведение проверки готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

-разрабатывает мероприятия по обеспечению безопасности персональных данных при обработке их в информационных системах персональных данных;

-разработке плана внутреннего контроля обработки персональных данных.

-проведению антивирусных мероприятий.

10.15.Для обеспечения внешней защиты персональных данных сотрудников осуществляется:

- порядок приема, учета и контроля деятельности посетителей;
- осуществление пропускного режима организации;
- учет и порядок выдачи пропусков;
- технические средства охраны -сигнализации, видеонаблюдения;

-охрана помещений и территории техникума сотрудниками охранной организации

- порядок охраны территории, зданий, помещений, транспортных средств.

10.16. С целью защиты персональных данных работников:

-хранение персональных данных (документов, материальных носителей персональных данных и др.) допускается только в помещениях оборудованных надежными замками и другими необходимыми средствами от несанкционированного проникновения; ключи от помещений, хранятся у ответственных за помещение лиц;

-запрещается:

- передача ключей неуполномоченным лицам;
- выдача личных дел сотрудников на рабочие места; личные дела могут выдаваться только директору, и в исключительных случаях, при подготовке документов на аттестацию работников, разрешается методисту произвести выписку необходимой информации в отделе кадров в присутствии работника отдела кадров;

-оставлять на рабочем месте без присмотра документы и другие материальные носители персональных данных;

- самостоятельное подключение неучтенных технических устройств и носителей информации, а также внесение изменений в программную среду вычислительной техники, применяемой для обработки персональных данных. При оставлении без

присмотра средств вычислительной техники, все учетные записи работника должны быть заблокированы.
- нахождение в помещении, в котором обрабатываются персональные данные посторонних лиц, не имеющих доступа к персональным данным, без присмотра.
-работникам учреждения, имеющим доступ к персональным данным, запрещена запись, хранение и вынос за пределы учреждения на внешних носителях информации (диски, дискеты, USB флэш-карты и т.п.), передача по внешним адресам электронной почты или размещение в сети Интернет информации, содержащей персональные данные субъектов без их согласия.

10.17. В случаях длительного отсутствия работника на своем рабочем месте (отпуск, командировка, болезнь), он обязан передать документы и иные носители, содержащие персональные данные работников лицу, на которое приказом, распоряжением будет возложено исполнение его трудовых обязанностей.
-в отсутствии работника на рабочем месте не должно быть документов, содержащих персональные данные субъектов ПДн
-в процессе работы документы, содержащие персональные данные, могут находиться на столах, в папках в течение рабочего дня. По окончании рабочего дня данные документы должны убираться в места постоянного хранения, исключающие к ним доступ третьих лиц. Персональный компьютер, на котором ведется обработка персональных данных должен быть защищен паролем, а при отсутствии работника на рабочем месте должен блокироваться;
-при уходе в отпуск, в иных случаях длительного отсутствия на рабочем месте, он обязан передать документы лицу, на которое локальным актом техникума будет возложено исполнение его трудовых обязанностей;

При увольнении работника, имеющего доступ к персональным данным субъектов ПДн, документы, и иные носители, содержащие персональные данные, передаются вновь назначенному на эту должность лицу;

Уборка помещений, в которых ведется обработка персональных данных, производится в присутствии работников.

10.18.Доступ в информационных системах персональных данных ограничивается только теми персональными данными, которые необходимы для выполнения трудовых функций конкретного работника.

10.19.Обработка персональных данных допускается только с применением учтенных средств вычислительной техники.

10.20.При передаче персональных данных третьей стороне должен использоваться безопасный канал передачи. Запрещается передавать персональные данные международного информационного обмена (отправлять по электронной почте и т.п.) без применения необходимых программных и/или аппаратных средств защиты.

11. Права Работников

11.1.В целях обеспечения безопасности персональных данных, хранящихся у Оператора Работники имеют право:
11.1.1. получать доступ к своим персональным данным и ознакомление с ними, включая право на безвозмездное получение копий любой записи, содержащей

персональные данные работника (за исключением случаев предусмотренных федеральным законом);
11.1.2. на получение информации, касающейся обработки его персональных данных, в том числе содержащей:
–подтверждение факта обработки персональных данных Оператором;
–правовые основания и цели обработки персональных данных;
–цели и применяемые Оператором способы обработки персональных данных;
–наименование и место нахождения Оператора, сведения о лицах (за исключением сотрудников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
–обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
–сроки обработки персональных данных, в том числе сроки их хранения;
–порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом "О персональных данных";
–информацию об осуществленной или о предполагаемой трансграничной передаче данных;
–наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка поручена или будет поручена такому лицу.
11.1.3.требовать от Работодателя уточнения, исключения или исправления неполных, неверных, устаревших, недостоверных, незаконно полученных или не являющих необходимыми для Работодателя персональных данных;
11.1.4. получать от Работодателя:
–сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
–перечень обрабатываемых персональных данных и источник их получения;
– сроки обработки персональных данных, в том числе сроки их хранения;
–сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой его отказ в предоставлении согласия на обработку персональных данных;
11.1.5.требовать извещения Работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях;
11.1.6.обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия Работодателя при обработке и защите его персональных данных.
11.1.7.Обращения субъектов персональных данных фиксируются в журналах обращений по ознакомлению с персональными данными, которые ведутся в структурных подразделениях техникума по форме, утвержденной приказом директора техникума (Приложение №9).
11.1.8.Ознакомление субъекта персональных данных с его персональными данными производится способом, исключающим разглашение персональных данных других субъектов персональных данных, кроме общедоступных.

12.Ответственность за нарушение норм, регулирующих порядок обработки и защиты персональных данных

12.1.Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с федеральными законами.

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

12.3.Должностные лица, в функции которых входит обработка персональных данных, несут персональную ответственность за нарушение порядка доступа работников техникума и третьих лиц к информации, содержащей персональные данные.

12.4.Сотрудник техникума, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

12.5. Разглашение персональных данных работника техникума, т.е.передача их посторонним лицам, в том числе, работникам, не имеющим к ним доступа, их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные работника, а также иные нарушения обязанностей по их защите и обработке, установленных настоящим Положением, локальными нормативными актами (приказами, распоряжениями) техникума, лицом, ответственным за получение, обработку и защиту персональных данных работника, влекут наложение на него дисциплинарного взыскания – замечания, выговора, увольнения.

12.6. В соответствии с Гражданским кодексом РФ лица, незаконными методами получившие информацию, составляющую персональные данные, обязаны возместить причиненные убытки; такая же обязанность возлагается и на работников, не обладающих правом доступа к персональным данным.

12.7.Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, а также требований к защите персональных данных, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

12.8. Сотрудники, имеющие доступ к персональным данным работника несут полную материальную ответственность в случае причинения его действиями ущерба работодателю. (п.7 ч.1 ст. 243 Трудового кодекса РФ).

12.9. Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения влечет наложение наказания в порядке, предусмотренном Уголовным кодексом РФ.