

УТВЕРЖДЕНО
приказом ГБПОУ УКРТБ
от «01» 09 2025 г. № 246/2к

**ПОЛОЖЕНИЕ
О ПОРЯДКЕ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ
В ГБПОУ УКРТБ**

1. Общие положения

1.1. Настоящее Положение разработано в целях защиты персональных данных работников, абитуриентов, обучающихся, законных представителей абитуриентов и обучающихся, контрагентов, с которыми заключены договорные отношения и иных физических лиц, персональные данные которых, обрабатываются для достижения уставных целей (далее – субъектов персональных данных) Государственного бюджетного образовательного учреждения «Уфимский колледж радиоэлектроники, телекоммуникаций и безопасности» (далее – учреждение, колледж, УКРТБ) от несанкционированного доступа, неправомерного их использования или утраты.

1.2. Настоящее Положение разработано в соответствии с требованиями Трудового кодекса РФ (далее - ТК), Федерального закона РФ от 27.07.2006 №152-ФЗ «О персональных данных», Постановления Правительства РФ от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», и определяет особенности обработки персональных данных работника.

1.3. Сбор, хранение, использование и распространение информации о частной жизни лица без письменного его согласия не допускаются. Персональные данные (далее – ПДн) относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75-летнего срока хранения, если иное не определено законом.

1.4. Должностные лица, в обязанность которых входит обработка персональных данных, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

1.5. Персональные данные не могут быть использованы в целях:

- причинения имущественного и морального вреда гражданам;
- затруднения реализации прав и свобод граждан Российской Федерации.

1.6. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с действующим законодательством.

1.7. Юридические и физические лица в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за распространение известных им персональных данных без согласия субъекта персональных данных, нарушение режима защиты, обработки и порядка использования этой информации.

1.8. Работники учреждения, обучающиеся, законные представители обучающихся, которым стали известны персональные данные, не вправе разглашать ее третьим лицам, в противном случае на них возлагается установленная законодательством ответственность. Неправомерность деятельности органов государственной власти и организаций по сбору персональных данных может быть установлена в судебном порядке по требованию субъектов согласно законодательству Российской Федерации.

1.9. Настоящее Положение утверждается директором, либо лицом, его замещающим и является обязательным для исполнения всеми работниками, имеющими доступ к обрабатываемым ПДн.

1.10. В настоящем Положении используются следующие основные понятия:

1.10.1. Персональные данные (ПД) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

1.10.2. 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 Федеральным законом № 152-ФЗ «О персональных данных».

1.10.3. 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.

1.10.4. 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.

1.10.5. Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

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

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

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

1.10.9. 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.

1.10.10. Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

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

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

1.10.13. Уровень защищенности персональных данных – комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных

угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

2. Состав персональных данных, подлежащих обработке в учреждении

2.1. Состав персональных данных работников:

- фамилия, имя, отчество;
- дата и место рождения;
- данные документа, удостоверяющего личность;
- идентификационный номер налогоплательщика;
- номер страхового свидетельства государственного пенсионного страхования (СНИЛС);
- номер полиса обязательного медицинского страхования;
- данные о регистрации по месту жительства или временного пребывания, данные о месте фактического проживания;
- доходы;
- банковские реквизиты;
- данные о профессии, занимаемой должности, образовании, квалификации и о наличии специальных знаний или специальной подготовки;
- данные о семейном положении (составе семьи);
- сведения о трудовом (страховом) стаже;
- сведения воинского учета;
- сведения о прохождении предварительных и периодических медицинских осмотров;
- сведения о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям;
- контактные телефоны.

К общедоступным сведениям относятся:

- фамилия, имя отчество;
- данные о профессии, занимаемой должности, квалификации;
- сведения о трудовом стаже.

2.3. Персональные данные обучающихся.

Состав персональных данных обучающихся:

- фамилия, имя отчество;
- дата и место рождения;
- гражданство;
- данные документа, удостоверяющего личность;
- идентификационный номер налогоплательщика;
- номер страхового свидетельства государственного пенсионного страхования (СНИЛС);
- номер полиса обязательного медицинского страхования;
- данные о регистрации по месту жительства или временного пребывания, данные о месте фактического проживания;
- сведения о стипендиях, социальных выплатах, иных доходах и выплатах;
- банковские реквизиты;
- данные о профессии, занимаемой должности, образовании, квалификации и о наличии специальных знаний или специальной подготовки;
- данные о семейном положении (составе семьи);
- сведения воинского учета;

- сведения о прохождении медицинских осмотров;
- сведения об образовании;
- сведения о месте работы;
- общественные поручения;
- увлечения и достижения;
- номер группы;
- характеристика;
- средний бал ЕГЭ;
- средний бал ОГЭ;
- район регистрации;
- код карты доступа;
- сведения о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям;
- характере взаимоотношений в семье;
- контактные телефоны.

К общедоступным сведениям относятся:

- фамилия, имя отчество;
- номер группы;
- успеваемость и посещаемость.

2.3. Персональные данные законных представителей абитуриентов и обучающихся.

Состав персональных данных:

- фамилия, имя отчество;
- степень родства;
- дата и место рождения;
- гражданство;
- данные документа, удостоверяющего личность;
- идентификационный номер налогоплательщика;
- номер страхового свидетельства государственного пенсионного страхования (СНИЛС);
- данные о регистрации по месту жительства или временного пребывания, данные о месте фактического проживания;
- сведения о месте работы;
- контактные телефоны.

К общедоступным сведениям относятся:

- фамилия, имя, отчество;
- степень родства.
- контактные телефоны.

2.4. Персональные данные контрагентов - физических лиц, с которыми заключены договорные отношения;

Состав персональных данных:

- фамилия, имя отчество;
- дата и место рождения;
- гражданство;
- данные документа, удостоверяющего личность;
- идентификационный номер налогоплательщика;
- номер страхового свидетельства государственного пенсионного страхования (СНИЛС);

- данные о регистрации по месту жительства или временного пребывания, данные о месте фактического проживания;
- сведения о доходах и выплатах;
- банковские реквизиты;
- сведения об образовании;
- контактные телефоны.

3. Перечень документов и сведений, содержащих персональные данные

3.1. В соответствии с ТК РФ, локальными нормативными актами учреждения лицо, поступающее на работу, предъявляет работодателю следующие документы, содержащие его персональные данные:

- паспорт или иной документ, удостоверяющий личность, содержащий сведения о паспортных данных работника, сведения о месте регистрации (месте жительства), сведения о семейном положении;
- трудовую книжку, содержащую данные о трудовой деятельности работника;
- страховое свидетельство государственного пенсионного страхования, содержащее сведения о номере и серии страхового свидетельства;
- свидетельство о постановке на учет в налоговом органе, содержащее сведения об идентификационном номере налогоплательщика;
- документы воинского учета, содержащие сведения о воинском учете военнообязанных и лиц, подлежащих призыву на военную службу;
- документ об образовании, о квалификации или о наличии специальных знаний или специальной подготовки, содержащий сведения об образовании, профессии;
- сведения о прохождении медицинского осмотра;
- справку, выданную органами МВД России, о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям (при поступлении на работу, к выполнению которой в соответствии с Трудовым кодексом РФ или иным федеральным законом не допускаются лица, имеющие или имевшие судимость, подвергающиеся или подвергавшиеся уголовному преследованию).

3.2. В перечень документов и сведений, содержащих персональные данные, включаются:

- трудовой договор;
- сведения о состоянии здоровья;
- личное дело, личная карточка работника;
- анкетные и паспортные данные;
- сведения о доходах;
- семейное, социальное, имущественное положение;
- образование;
- трудовая книжка;
- доверенности;
- справка, выданная органами МВД России, о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям;
- комплекты документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении;

- комплект материалов по анкетированию, тестированию, проведению собеседований с кандидатом на должность;

- подлинники и копии приказов (распоряжений) по кадрам;
- дела, содержащие основания к приказу по личному составу;
- дела, содержащие материалы аттестаций работников;
- дела, содержащие материалы внутренних расследований;
- справочно-информационный банк данных по работникам (картотеки, журналы);
- подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству Компании, руководителям структурных подразделений;
- копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения.

3.3. При поступлении в учреждение абитуриенты/обучающиеся либо их законные представители предоставляют следующие документы:

- документ, удостоверяющий личность;
- документ о получении образования;
- индивидуальный номер налогоплательщика;
- полис обязательного медицинского страхования
- сведения о воинском учете;
- сведения о прохождении медицинского осмотра.

3.4. В перечень документов и сведений, содержащих персональные данные обучающихся, включаются:

- личная карточка;
- договор на оказание платных образовательных услуг;
- анкета;
- журнал классного руководителя;
- характеристика;
- личное дело;
- справочно-информационный банк данных по обучающимся (картотеки, журналы).

4. Требования по обработке персональных данных

4.1. В целях обеспечения прав и свобод человека и гражданина учреждения, являющийся оператором персональных данных (далее по тексту – Оператор) и его представители при обработке персональных данных обязаны соблюдать следующие общие требования:

- обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности, контроля количества и качества выполняемой работы, для определения возможности зачисления абитуриента для дальнейшего обучения, осуществления контроля за образовательным процессом студента, обеспечения сохранности имущества и иных целей, указанных в уставе колледжа, исполнения договоров;

- при определении объема и содержания обрабатываемых персональных данных Оператор должен руководствоваться Конституцией РФ, ТК РФ и иными федеральными законами;

- все персональные данные субъекта персональных данных (работника, абитуриента, обучающегося, контрагента, законных представителей) следует получать у него самого, а если

субъект является несовершеннолетним – возможно получение данных от его законного представителя.

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

Защита персональных данных от неправомерного их использования или утраты должна быть обеспечена Оператором за счет своих средств в порядке, установленном федеральным законом.

Субъекты персональных данных должны быть ознакомлены под роспись с документами организации, устанавливающими порядок обработки персональных данных, а также об их правах и обязанностях в этой области.

5. Обязанности субъектов персональных данных

5.1. Субъект персональных данных обязан:

5.1.1. Передавать Оператору или его представителю комплект достоверных, документированных персональных данных, состав которых установлен законодательством, внутренними локальными актами Оператора.

5.1.2. Своевременно сообщать Оператору об изменении своих персональных данных.

6. Права субъектов персональных данных

6.1. Субъект персональных данных имеет право:

- на получение полной информации о своих персональных данных и обработке 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 работников 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 федеральными законами;

- 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;

- иные сведения, предусмотренные федеральными законами;

- требовать уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

- заявить в письменной форме о несогласии с решением, принятым на основании исключительно автоматизированной обработки его персональных данных;
- обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

6.2. Субъект персональных данных не должен отказываться от своих прав на сохранение и защиту тайны.

7. Сбор, обработка и хранение персональных данных

7.1. Порядок получения персональных данных:

7.1.1. Все персональные данные субъекта персональных данных следует получать у него самого. Если персональные данные возможно получить только у третьей стороны, то субъект персональных данных должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Оператор должен сообщить субъекту персональных данных 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.

7.1.2. Оператор не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях, и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции РФ Оператор вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

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

7.1.4. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в пунктах 2, 3, 4, 8 части 1 статьи 6 Федерального закона «О персональных данных».

7.2. Обработка, передача и хранение персональных данных:

7.2.1. К обработке, передаче и хранению персональных данных могут иметь доступ работники следующих структурных подразделений учреждения:

- бухгалтерии;
- отдела кадров;
- вычислительного центра;
- учебно-методического отдела;
- отдела по воспитательной работе;
- библиотеки;
- члены приемной комиссии
- иные работники.

7.2.2. Круг лиц, допущенных к работе с документами, содержащими персональные данные, определяется приказом директора, либо лицом, его замещающим.

7.3. При передаче персональных данных Оператор должен соблюдать следующие требования:

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

- не сообщать персональные данные в коммерческих целях без его письменного согласия;

- предупредить лиц, получающих персональные данные, 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, получающие персональные данные, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными в порядке, установленном федеральными законами;

- разрешать доступ к персональным данным только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций;

- не запрашивать информацию о состоянии здоровья, за исключением тех сведений, которые относятся к вопросу о возможности выполнения трудовой функции, возможности участвовать в образовательном процессе;

- опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему политику Оператора в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных.

7.4. Передача персональных данных от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

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

7.6. Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу. Допускается выдача информации о персональных данных по письменному запросу субъекта персональных данных путем направления запрашиваемых им сведений путем почтового отправления.

7.7. С работниками, допущенными к обработке персональных данных, заключаются Соглашения о неразглашении персональных данных. Экземпляр Соглашения хранится в отделе кадров.

7.8. Автоматизированная обработка и хранение персональных данных допускаются только при условии выполнения всех основных мероприятий по защите информации.

7.9. Помещения, в которых хранятся персональные данные, должны быть оборудованы надежными запорными устройствами.

7.10. Помещения в рабочее время при отсутствии в них работников отделов должны быть закрыты.

7.11. Проведение уборки помещения должно производиться в присутствии работников отделов, имеющих доступ к персональным данным.

8. Доступ к персональным данным

8.1. Право доступа к персональным данным имеют:

- директор, либо лицо, его замещающее;
- лица, в соответствии с внутренними локальными актами.

8.2. Внешний доступ.

8.2.1. К числу массовых потребителей персональных данных вне колледжа относятся государственные и негосударственные функциональные структуры:

- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- страховые агентства, осуществляющие обязательное страхование;
- военные комиссариаты;
- органы социального страхования;
- пенсионные фонды;
- подразделения муниципальных органов управления.

В указанные структуры передача персональных данных допускается только в случаях соответствия целям обработки данных.

8.2.2. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

8.2.3. Организации, в которые субъект персональных данных может осуществлять перечисления денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к его персональным данным только в случае его письменного разрешения.

8.2.4. Сведения о работающем работнике или уже уволенном, об абитуриенте, о студенте, обучающемся либо прекратившем обучение, могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии нотариально заверенного заявления субъекта персональных данных.

8.2.5. Персональные данные субъекта могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого субъекта персональных данных, если субъектом персональных данных является лицо, не достигшее совершеннолетия, данные могут быть выданы без его согласия законным представителям.

9. Защита персональных данных

9.1. Учреждение обязано при обработке персональных данных принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

9.2. Защите подлежат:

- персональные данные на бумажных носителях;
- персональные данные на электронных носителях.

9.3. В систему защиты персональных данных входят:

- директор, либо лицо, его замещающее;
- ответственный за организацию обработки персональных данных;
- начальник отдела кадров;
- главный бухгалтер;
- члены приемной комиссии;
- администратор информационных систем персональных данных (ИСПДн).

9.3.1. Директор, либо лицо, его замещающее отвечает за:

- проведение единой политики и координацию работ по организации обработки и обеспечению безопасности персональных данных;

- организацию в учреждении режима конфиденциальности персональных данных.

9.3.2. Ответственный за организацию обработки персональных данных отвечает за:

- планирование и проведение мероприятий по организации обеспечения безопасности персональных данных;
- постоянный контроль за обеспечением требований безопасности персональных данных;
- контроль за исполнением организационных распорядительных документов по организации обработки и обеспечению безопасности персональных данных;
- подготовку предложений по совершенствованию системы защиты персональных данных;
- организацию повышения осведомленности работников учреждения по вопросам обеспечения безопасности персональных данных.

9.3.3. Начальник отдела кадров обеспечивает:

- ознакомление работников под роспись с настоящим Положением, приказами и иными внутренними локальными нормативными актами, регулирующими обработку и защиту персональных данных;
- истребование с работников письменного обязательства о соблюдении конфиденциальности персональных данных и соблюдении правил их обработки (приведено в Приложение №1);
- общий контроль соблюдения работниками мер по защите персональных данных;
- хранение личных дел и документов, содержащих персональные данные, в запирающихся шкафах (сейфах), обеспечивающих защиту от несанкционированного доступа;
- выдачу личных дел только по письменному разрешению директора, либо лица, его замещающего, руководителям структурных подразделений (например, при подготовке материалов для аттестации работника);
- недопущение выдачи личных дел на рабочие места руководителей (личные дела могут выдаваться на рабочие места только директору);
- контроль возврата в отдел кадров в конце рабочего дня всех выданных работникам документов, содержащий ПДн;
- организацию обучения работников отдела кадров требованиям российского законодательства в области обработки ПДн.

9.3.4. Руководители структурных подразделений, указанные в п. 7.2.1. обеспечивают:

- контроль за соблюдением подчиненными работниками требований по защите персональных данных;
- осуществление хранения документов, содержащих персональные данные в запирающихся шкафах (сейфах), обеспечивающих защиту от несанкционированного доступа;
- организацию обучения подчиненных работников требованиям российского законодательства в области обработки ПДн.

9.3.5. Члены приемной комиссии обеспечивают:

- ознакомление абитуриентов, законных представителей абитуриентов под роспись с настоящим Положением, приказами и иными внутренними локальными нормативными актами, в т.ч. регулирующими обработку и защиту персональных данных в учреждении;
- хранение личных дел и документов, содержащих персональные данные обучающихся, законных представителей обучающихся, в запирающихся шкафах (сейфах), обеспечивающих защиту от несанкционированного доступа;
- выдачу личных дел только по письменному разрешению директора, либо лица, его замещающего, руководителям структурных подразделений.

9.3.6. Администратор информационных систем персональных данных (ИСПДн) обеспечивает:

- выполнение требований действующих нормативных и руководящих документов, а также внутренних локальных нормативных актов, регламентирующих порядок действий по защите информации;
- установку, настройку и своевременное обновление элементов ИСПДн (прикладного и специального программного обеспечения, средств защиты информации), функционирование и поддержку работоспособности средств защиты;
- работоспособность элементов ИСПДн и локальной вычислительной сети;
- контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов;
- контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов\$
- контроль за правильностью использования персональных паролей;
- своевременное принятие мер по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

9.4. Все работники, допущенные к обработке персональных данных, на основании письменного обязательства несут персональную ответственность за соблюдение конфиденциальности персональных данных.

9.5. Работники, допущенные к обработке персональных данных, обязаны соблюдать следующие правила:

- обеспечивать хранение информации, содержащей персональные данные, исключаящее доступ к ним третьих лиц;
- в отсутствие работника на его рабочем месте не должно быть документов, содержащих персональные данные;
- при уходе в отпуск, во время служебной командировке и иных случаях длительного отсутствия работника на своем рабочем месте, передать документы и иные носители, содержащие персональные данные лицу, на которое приказом или распоряжением директора, либо лица, его замещающего, будет возложено исполнение его трудовых обязанностей.

В случае если такое лицо не назначено, то документы и иные носители, содержащие персональные данные, передаются другому работнику, имеющему доступ к персональным данным по письменному распоряжению руководителя структурного подразделения.

При увольнении работника, имеющего доступ к персональным данным, документы и иные носители, содержащие персональные данные, передаются другому работнику, имеющему доступ к персональным данным по указанию директора, либо лица, его замещающего.

Допуск к персональным данным других работников учреждения, не имеющих надлежащим образом оформленного доступа, запрещается.

Копировать и делать выписки персональных данных разрешается исключительно в служебных целях при наличии письменного разрешения директора, либо лица его замещающего.

9.6. Защита информационных систем учреждения, в которых обрабатываются персональные данные, от несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке, осуществляется на основании законодательства РФ, нормативных актов ФСТЭК и ФСБ России, а также внутренних локальных нормативных актов, в соответствии с установленным уровнем защищенности.

Защита электронных носителей, содержащих персональные данные, обеспечивается, том числе путем:

- ограничения доступа в помещения, где расположены основные элементы информационных систем персональных данных;
- использования лицензированных антивирусных и антихакерских программ, не допускающих несанкционированный доступ к персональным данным;
- разграничения прав доступа с использованием учетной записи;
- установления правил разграничения 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;
- учета машинных носителей персональных данных;
- обнаружения фактов несанкционированного доступа к персональным данным и принятием соответствующих мер;
- контроля эффективности принимаемых мер по обеспечению защищенности персональных данных.

9.6. Все информационные ресурсы, содержащие персональные данные, должны быть недоступны для иных работников, не имеющих доступ к персональным данным.

9.7. Для защиты персональных данных необходимо выполнение ряда мер:

- установление порядка охраны территории, зданий, помещений;
- определения порядка доступа на объекты колледжа;
- оборудование помещений, в которых ведется обработка персональных данных, техническими средствами охраны и пожарной сигнализацией;
- принятия достаточных мер по защите информации при обработке персональных данных, в том числе с использованием средств автоматизации;
- соблюдения требований безопасности информации при обработке персональных данных;
- выполнение требований к защите информации при интервьюировании и собеседованиях.

10. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника

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

10.1. Руководитель, разрешающий доступ работника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

10.2. Каждый работник, получающий для работы конфиденциальный документ либо имеющий доступ к электронным базам данных, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

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

- дисциплинарную (замечание, выговор, увольнение);
- административную (предупреждение или административный штраф);
- гражданско-правовую (возмещение причиненного ущерба).

10.4. Субъект персональных данных, предоставивший Оператору подложные документы или заведомо ложные сведения о себе, несет дисциплинарную, административную, уголовную ответственность.

11. Заключительные положения

11.1. Настоящее Положение вступает в силу с момента его утверждения.

11.2. Положение обязательно для всех субъектов персональных данных учреждения, если иные условия не предусмотрены в трудовом договоре работника, соглашении с абитуриентами, студентами.

Разработал:

Заведующий лабораторией



Семенов А.Г.

Согласовано:

Начальник отдела кадров

Юрисконсульт



Леонтьева В.А.



Лукашова О.В.

Приложение №1
к Положению о порядке обработки
персональных данных в ГБПОУ УКРТБ

ОБЯЗАТЕЛЬСТВО

о неразглашении персональных данных работника, обучающегося, законного представителя обучающегося

Я, _____, паспорт серии _____, номер _____, выданный
_____ «___» _____ года, должность _____
_____ понимаю, что получаю
доступ к персональным данным работников (в том числе контрагентов, оформленных по
договорам гражданско-правового характера), абитуриентов, обучающихся, законных
представителей обучающихся (далее – субъектов персональных данных) в ГБПОУ УКРТБ. Я
также понимаю, что во время исполнения своих обязанностей мне приходится заниматься сбором,
обработкой и хранением персональных данных работников, обучающихся, законных
представителей обучающихся.

Я понимаю, что разглашение такого рода информации может нанести ущерб субъектам
персональных данных, как прямой, так и косвенный.

В связи с этим даю обязательство при работе (сборе, обработке и хранении) с
персональными данными субъектов персональных данных соблюдать все требования
действующего законодательства и внутренних локально-правовых актов в части обеспечения
безопасности персональных данных.

Я подтверждаю, что не имею права разглашать сведения о (об):

1. Персональных данных работника:

- фамилия, имя, отчество;
- дата и место рождения;
- данные документа, удостоверяющего личность;
- идентификационный номер налогоплательщика;
- номер страхового свидетельства государственного пенсионного страхования (СНИЛС);
- номер полиса обязательного медицинского страхования;
- данные о регистрации по месту жительства или временного пребывания, данные о месте фактического проживания;
- доходы;
- банковские реквизиты;
- данные о профессии, занимаемой должности, образовании, квалификации и о наличии специальных знаний или специальной подготовки;
- данные о семейном положении (составе семьи);
- сведения о трудовом (страховом) стаже;
- сведения воинского учета;
- сведения о прохождении предварительных и периодических медицинских осмотров;
- сведения о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям;
- контактные телефоны.

2. Персональных данных абитуриентов, обучающихся:

- фамилия, имя отчество;

- дата и место рождения;
- гражданство;
- данные документа, удостоверяющего личность;
- идентификационный номер налогоплательщика;
- номер страхового свидетельства государственного пенсионного страхования (СНИЛС);
- номер полиса обязательного медицинского страхования;
- данные о регистрации по месту жительства или временного пребывания, данные о месте фактического проживания;
- сведения о стипендиях, социальных выплатах, иных доходах и выплатах;
- банковские реквизиты;
- данные о профессии, занимаемой должности, образовании, квалификации и о наличии специальных знаний или специальной подготовки;
- данные о семейном положении (составе семьи);
- сведения воинского учета;
- сведения о прохождении медицинских осмотров;
- сведения об образовании;
- сведения о месте работы;
- общественные поручения;
- увлечения и достижения;
- номер группы;
- характеристика;
- средний бал ЕГЭ;
- средний бал ОГЭ;
- район регистрации;
- код карты доступа;
- сведения о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям;
- характере взаимоотношений в семье;
- контактные телефоны.

3. Персональных данных законных представителей:

- фамилия, имя отчество;
- степень родства;
- дата и место рождения;
- гражданство;
- данные документа, удостоверяющего личность;
- идентификационный номер налогоплательщика;
- номер страхового свидетельства государственного пенсионного страхования (СНИЛС);
- данные о регистрации по месту жительства или временного пребывания, данные о месте фактического проживания;
- сведения о месте работы;
- контактные телефоны

Настоящим добровольно принимаю на себя обязательства:

- не передавать (в любом виде) и не разглашать третьим лицам, работникам и обучающимся учреждения, не имеющим на это право в силу выполняемых ими должностных обязанностей или в соответствии с решением руководителя, информацию, содержащую персональные данные

субъектов персональных данных (за исключением собственных данных), которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей;

- в случае попытки третьих лиц, работников или обучающихся учреждения, не имеющих на это право, получить от меня информацию, содержащую персональные данные, немедленно сообщать об этом факте своему непосредственному или (в случае отсутствия непосредственного) вышестоящему руководителю;

- не использовать информацию, содержащую персональные данные, с целью получения выгоды;

- выполнять требования закона и иных нормативных правовых актов Российской Федерации, а также внутренних документов организации, регламентирующих вопросы защиты интересов субъектов персональных данных, порядка обработки и защиты персональных данных;

- после прекращения моих прав на доступ к информации, содержащей персональные данные (переход на должность, не предусматривающую доступ к персональным данным, или прекращения трудового договора), не обрабатывать, не разглашать и не передавать третьим лицам и не уполномоченным на это служащим организации, известную мне информацию, содержащую персональные данные;

- в случае расторжения со мной трудового договора прекратить обработку персональных данных, ставших мне известными в связи с исполнением должностных обязанностей, имеющиеся документы, содержащие персональные данные, передать не позднее дня прекращения трудового договора.

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

С Положением о порядке обработки персональных данных ГЫПОУ УКРТБ и гарантиях их защиты ознакомлен(а).

«___» _____ 20__ г.

_____/_____
(подпись)