1

# ПОЛИТИКА

**обработки и защиты персональных данных
в краевом государственном автономном
профессиональном образовательном учреждении
«Дальнегорский индустриально-технологический колледж»**

СОГЛАСОВАНО
заседанием педагогического Совета
Протокол № 1 от «31» августа 2020 г.

УТВЕРЖДАЮ
Директор КГА ПОУ «ДИТК»
Матвеева В.Г. _____
«31» августа 2020 г.

г. Дальнегорск

2020 г.

# СОДЕРЖАНИЕ


1. ОСНОВНЫЕ ПОЛОЖЕНИЯ…… 3
2. ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ…… 5
3. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ…… 6
4. ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ, СОСТАВЛЯЮЩЕЙ ПЕРСОНАЛЬНЫЕ ДАННЫЕ…… 10
5. ОСНОВНЫЕ ТРЕБОВАНИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ, СОСТАВЛЯЮЩЕЙ ПЕРСОНАЛЬНЫЕ ДАННЫЕ..... 14
6. ПРАВА СУБЪЕКТОВ……. 17
7. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ СУБЪЕКТА…… 19
8. ПОРЯДОК ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ЭКСПЛУАТАЦИИ ИСПДН…… 20
9. КОНТРОЛЬ СОСТОЯНИЯ И ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИСПДН…… 21
10. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ И НАРУШЕНИЕ…… 23

# 1. ОСНОВНЫЕ ПОЛОЖЕНИЯ

Настоящая Политика разработана на основании:

- Конституции РФ;

- Гражданского Кодекса РФ;

- Трудового Кодекса РФ, и в соответствии с требованиями:

- Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных»;

- Постановления Правительства РФ от 21.03.2012 N 211"Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами".

Цель данной Политики – обеспечение прав граждан при обработке их персональных данных, и принятие мер от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных Субъектов.

1.1. Настоящая Политика устанавливает порядок организации и проведения работ по защите информации в информационной системе персональных данных, создаваемых и эксплуатируемых в колледже.

1.2. Требования настоящей Политики распространяются на защиту информации с ограниченным доступом, отнесенной к информации, составляющей персональные данные.

1.3. Политика является дополнением к действующим в РФ нормативным документам по вопросам обеспечения информационной безопасности персональные данные, и не исключает обязательного выполнения их требований.

1.4. Политика служит основой для разработки комплекса организационных и технических мер по обеспечению информационной

безопасности персональных данных колледжа, а также нормативных и методических документов, обеспечивающих ее реализацию.

1.5. Юридические и физические лица, в соответствии со своими полномочиями, владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

1.6. Настоящая политика утверждается директором КГА ПОУ «Дальнегорский индустриально-технологический колледж» и является обязательным для исполнения всеми сотрудниками, имеющими доступ к персональным данным Субъекта.

## 2. ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

**ИСПДн** – информационная система персональных данных.

**НСД** - несанкционированный доступ.

**ПДн** – персональные данные.

**Политика** – политика образовательной организации в отношении обработки персональных данных.

**СЗПДн** – система защиты персональных данных.

**ТЗКИ** – техническая защита конфиденциальной информации.

**ТС** – техническое средство.

**Колледж** – краевое государственное автономное профессиональное образовательное учреждение «Дальнегорский индустриально-технологический колледж».

# 3. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

**Безопасность информации** – состояние защищенности информации, характеризуемое способностью технических средств и информационных технологий обеспечивать конфиденциальность, целостность и доступность информации при ее обработке техническими средствами.

**Вирус** (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

**Вредоносная программа** – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

**Доступ к информации** – возможность получения информации и ее использования.

**Защищаемая информация** – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

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

**Источник угрозы безопасности информации** – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

**Накопитель информации** – устройство, предназначенное для записи и (или) чтения информации на носитель информации. Накопитель информации конструктивно может содержать в себе неотчуждаемый носитель информации, либо может быть предназначен для использования сменных носителей информации. Накопители подразделяются на встроенные (в конструктиве системного блока) и внешние (подсоединяемые через порт). Встроенные накопители подразделяются на съемные и несъемные.

**Нарушитель безопасности персональных данных** – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке (в том числе техническими средствами) в информационных системах персональных данных.

**Несанкционированный доступ** (несанкционированные действия) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своему функциональному предназначению и техническим характеристикам.

**Носитель информации** – физический объект, предназначенный для хранения информации.

**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.

**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.

**Перехват** (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

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

**Пользователь информационной системы персональных данных** – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

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

**Система защиты персональных данных** – комплекс организационных мер и программно-технических (в том числе криптографических) средств обеспечения безопасности информации в ИСПДн.

**Технические средства информационной системы персональных данных** - средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации.

**Технический канал утечки информации** – совокупность носителя информации (средства обработки), физической среды распространения

информативного сигнала и средств, которыми добывается защищаемая информация.

**Угрозы безопасности персональных данных** – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе 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.

**Утечка (защищаемой) информации по техническим каналам** – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

# 4. ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ, СОСТАВЛЯЮЩЕЙ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

4.1 Персональные данные могут обрабатываться только в целях, непосредственно связанных с деятельностью колледжа, в частности для:

- обеспечения соблюдения Конституции Российской Федерации, законодательных и иных нормативных правовых актов Российской Федерации, локальных нормативных актов Колледжа;
- осуществления функций, полномочий и обязанностей, возложенных законодательством Российской Федерации на Колледж, в том числе по предоставлению персональных данных в органы государственной власти, в Пенсионный фонд Российской Федерации, в Фонд социального страхования Российской Федерации, в Федеральный фонд обязательного медицинского страхования, их территориальные представительства и подразделения, а также в иные государственные органы;
- осуществления образовательной и воспитательной программ колледжа;
- проведения и(или) участия сотрудников, студентов колледжа в олимпиадах, семинарах, конкурсах, форумах, соревнованиях, состязаниях, смотрах, выставках;
- направление сотрудников на обучение;
- направление работ сотрудников, студентов на конкурсы;
- дистанционного обучения;
- ведения электронного дневника и электронного журнала успеваемости;
- автоматизации работы библиотеки, проведения мониторинга образовательной деятельности.
- ведения финансово-хозяйственной деятельностью колледжа;
- в иных случаях предусмотренных законодательством РФ
- социальной защиты сотрудников и студентов колледжа.

4.2 Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации.

4.3 Защита информации, составляющей ПДн должна осуществляться в соответствии со следующими основными принципами:

**Законность** - предполагает обеспечение защиты ПДн в соответствии с действующим в РФ законодательством и нормативными актами в области защиты ПДн. Пользователи и обслуживающий персонал ИСПДн должны быть осведомлены о правилах и порядке работы с защищаемой информацией и об ответственности за их нарушение.

**Системность** - предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности ПДн ИСПДн.

**Комплексность** - предполагает согласованное применение разнородных средств и систем при построении комплексной системы защиты информации, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Для каждого канала утечки информации и для каждой угрозы безопасности должно существовать несколько защитных рубежей. Создание защитных рубежей осуществляется с учетом того, чтобы для их преодоления потенциальному злоумышленнику требовались профессиональные навыки в нескольких невзаимосвязанных областях.

**Непрерывность** - предполагает функционирование СЗПДн в виде непрерывного целенаправленного процесса, предполагающего принятие соответствующих мер на всех этапах жизненного цикла ИСПДн. ИСПДн должны находиться в защищенном состоянии на протяжении всего времени их функционирования. В соответствии с этим принципом должны приниматься меры, не допускающие переход ИСПДн в незащищенное состояние.

**Своевременность** - предполагает упреждающий характер мер обеспечения безопасности ПДн, то есть постановку задач по комплексной защите ИСПДн и реализацию мер обеспечения безопасности ПДн на ранних стадиях разработки ИСПДн в целом и ее системы защиты информации, в частности.

**Совершенствование** - предполагает постоянное совершенствование мер и средств защиты информации на основе комплексного применения организационных и технических решений, квалификации персонала, анализа функционирования ИСПДн и ее системы защиты с учетом изменений условий функционирования ИСПДн, появления новых методов и средств перехвата информации, изменений требований нормативных документов по защите ПДн.

**Персональная ответственность** - предполагает возложение ответственности за обеспечение безопасности ПДн и ИСПДн на каждого исполнителя в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей исполнителей строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

**Минимальная достаточность** - предполагает предоставление исполнителям минимально необходимых прав доступа к ресурсам ИСПДн в соответствии с производственной необходимостью, на основе принципа «запрещено все, что не разрешено явным образом».

**Гибкость системы защиты** - предполагает наличие возможности варьирования уровнем защищенности при изменении условий функционирования ИСПДн.

**Обязательность контроля** - предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности ПДн на основе используемых систем и средств защиты информации. Контроль деятельности каждого пользователя, каждого средства защиты и в отношении каждого

объекта защиты должен осуществляться на основе применения средств контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

# 5. ОСНОВНЫЕ ТРЕБОВАНИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ, СОСТАВЛЯЮЩЕЙ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

5.1 Обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных, если иное не предусмотрено законодательством Российской Федерации в области персональных данных.

5.2 Колледж без согласия субъекта персональных данных не раскрывает третьим лицам и не распространяет персональные данные, если иное не предусмотрено федеральным законом.

5.3 Колледж вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных на основании заключаемого с этим лицом договора. Договор должен содержать перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, цели обработки, обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона «О персональных данных».

5.4 В целях внутреннего информационного обеспечения Колледжем может создавать внутренние справочные материалы, в которые с письменного согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации, могут включаться его фамилия, имя, отчество, место работы, место учебы, должность, год и место рождения, адрес, абонентский номер, адрес электронной почты, иные персональные данные, сообщаемые субъектом персональных данных.

5.5 Доступ к обрабатываемым в Колледже персональным данным разрешается только работникам Колледжа, занимающим должности,

включенные в перечень должностей, при замещении которых осуществляется обработка персональных данных.

5.6 Режим конфиденциальности ПДн снимается в случаях обезличивания или включения их в общедоступные источники ПДн, если иное не определено законом.

5.7Защита персональных данных представляет собой жестко регламентированный и динамически технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и учебно-воспитательной деятельности колледжа.

5.8 Регламентация доступа сотрудников колледжа к документам и базам данных с персональными сведениями входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий руководителями и сотрудниками колледжа. Для защиты персональных данных субъектов необходимо соблюдать ряд мер:

- осуществление пропускного режима в служебные помещения;
- назначение должностных лиц, допущенных к обработке ПД;
- хранение ПД на бумажных носителях в охраняемых или запираемых помещениях, сейфах, шкафах;
- наличие необходимых условий в помещении для работы с документами и базами данных с персональными сведениями;
- в помещение, в котором находится вычислительная техника;
- организация порядка уничтожения информации;
- ознакомление работников, непосредственно осуществляющих обработку ПДн, с требованиями законодательства РФ в сфере ПДн, локальными актами оператора в сфере ПДн и обучение указанных работников.
- осуществление обработки ПДн в ИСПДн на рабочих местах с разграничением полномочий, ограничение доступа к рабочим местам,

применение механизмов идентификации доступа по паролю и электронному ключу, средств криптозащиты;

- осуществление внутреннего контроля соответствия обработки ПДн требованиям законодательства.

5.9 Для защиты персональных данных создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

5.10 Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности колледжа, посетители, работники других организационных структур.

5.11 Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов, содержащих ПДн.

5.12 Для защиты ПДн Субъектов необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;
- технические средства охраны, сигнализации;
- порядок охраны помещений, транспортных средств;
- требования к защите информации, предъявляемые соответствующими нормативными документами.

## 6. ПРАВА СУБЪЕКТОВ

В Колледже обрабатываются персональные данные следующих категорий субъектов: работники структурных подразделений Колледжа, его филиалов и отделений; обучающиеся Колледжа; другие субъекты персональных данных.

6.1 Право на доступ к информации о самом себе. Право Субъекта на доступ к своим персональным данным ограничивается в случае, если предоставление персональных данных нарушает конституционные права и свободы других лиц. Сведения о наличии персональных данных должны быть предоставлены Субъекту в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

6.2 Право на определение форм и способов обработки персональных данных.

6.3 Право на отзыв согласия на обработку персональных данных.

6.4 Право ограничивать способы и формы обработки персональных данных, запрет на распространение персональных данных без его согласия.

6.5 Право требовать изменение, уточнение, уничтожение информации о самом себе.

6.6 Право обжаловать неправомерные действия или бездействия по обработке персональных данных и требовать соответствующей компенсации в суде.

6.7 Право на дополнение персональных данных оценочного характера заявлением, выражающим его собственную точку зрения.

6.8 Право определять представителей для защиты своих персональных данных.

6.9 Право требовать от колледжа уведомления всех лиц, которым ранее были сообщены неверные или неполные персональные данные Субъекта, обо всех произведенных в них изменениях или исключениях из них.

6.10 Персональные данные Субъекта могут быть предоставлены третьим лицам только с письменного согласия Субъекта, кроме случаев, связанных с выполнением требований законодательств РФ.

## 7. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ СУБЪЕКТА

7.1. Доступ Субъекта к своим персональным данным предоставляется при обращении либо при получении запроса Субъекта. Колледж обязан сообщить Субъекту информацию о наличии персональных данных о нем, а также предоставить возможность ознакомления с ними в течение тридцати рабочих дней с момента обращения или получения запроса.

7.2. Запрос должен содержать номер основного документа, удостоверяющего личность Субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись Субъекта персональных данных или его законного представителя. Запрос может быть направлен в электронной форме и подписан электронной цифровой подписью в соответствии с законодательством Российской Федерации.

7.3. Субъект имеет право на получение при обращении или при получении запроса информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных колледжем, а также цель такой обработки;
- способы обработки персональных данных, применяемые колледжем;
- 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 может повлечь за собой обработка его персональных данных.

# 8. ПОРЯДОК ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ЭКСПЛУАТАЦИИ ИСПДН

8.1. Эксплуатация информационной системы персональных данных должна осуществляться в полном соответствии с утвержденной проектной, организационно-распорядительной и эксплуатационной документацией информационной системы персональных данных.

8.2. Ответственность за обеспечение защиты информации в процессе эксплуатации информационной системы персональных данных возлагается на заместителя директора колледжа, в ведении которой находится эта информационная система персональных данных.

8.3. Ответственность за соблюдение установленных требований по защите информации при ее обработке в информационной системы персональных данных возлагается на непосредственных исполнителей информационной системы персональных данных (пользователей, администраторов, обслуживающий персонал).

8.4. За нарушение установленных требований по защите информации заместитель директора колледжа, в ведении которой находится информационная система персональных данных, и (или) непосредственный исполнитель привлекаются к ответственности в соответствии с действующим в РФ законодательством.

# 9. КОНТРОЛЬ СОСТОЯНИЯ И ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПРЕСОНАЛЬНЫХ ДАННЫХ

9.1. В информационной системе персональных данных должен осуществляться контроль и (или) аудит соответствия обработки персональных данных действующим в РФ законодательству и требованиям к защите персональных данных, а так же настоящей Политике и локальным актам колледжа.

9.2. Контроль заключается в оценке выполнения требований нормативных документов, обоснованности принятых мер и оценке эффективности принятых мер по обеспечению персональных данных.

9.3. Контроль подразделяется на оперативный и плановый (периодический).

9.4. В процессе эксплуатации информационной системе персональных данных в целях защиты информации от несанкционированного доступа осуществляются оперативный контроль и периодический контроль за выполнением исполнителями требований действующих нормативных документов по вопросам обеспечения безопасности и защиты персональных данных.

9.5. С целью своевременного выявления и предотвращения утечки информации, исключения или существенного затруднения несанкционированного доступа и предотвращения специальных воздействий (программно-технических и др.), вызывающих нарушение целостности информации или работоспособность технических средств, в информационной системе персональных данных колледжа проводится плановый периодический (не реже одного раза в год) контроль состояния защиты информации.

9.6. При проведении плановых проверок осуществляется контроль ведения учетной документации, защищенности информационной системы персональных данных от утечки персональных данных по техническим

каналам, выборочный контроль содержимого накопителей и носителей информации, и т.п.

9.7 Внутренний контроль за соблюдением законодательства Российской Федерации и локальных нормативных актов в области персональных данных, в том числе требований к защите персональных данных, осуществляется лицом, ответственным за организацию обработки персональных данных.

9.8 Внутренний контроль соответствия обработки персональных данных Федеральному закону «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, настоящей Политике, локальным нормативным актам Колледжа осуществляет отдел кадров Колледжа (по работникам) и учебная часть (по обучающимся).

9.10 Результаты контроля оформляются актами, заключениями и записями в эксплуатационной документации.

## 10. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ И НАРУШЕНИЕ

10.1. Колледж ответственен за персональную информацию, которая находится в его распоряжении и закрепляет персональную ответственность сотрудников за соблюдением, установленных в организации принципов уважения приватности.

10.2.Каждый сотрудник колледжа, получающий для работы доступ к материальным носителям персональным данных, несет ответственность за сохранность носителя и конфиденциальность информации.

10.3.Колледж обязуется поддерживать систему приема, регистрации и контроля рассмотрения жалоб Субъектов, доступную как посредством использования Интернета, так и с помощью телефонной, телеграфной или почтовой связи.

10.4.Любое лицо может обратиться к сотруднику колледжа с жалобой на нарушение данной Политики. Жалобы и заявления по поводу соблюдения требований обработки данных рассматриваются в течение тридцати рабочих дней с момента поступления.

10.5.Сотрудники колледжа обязаны на должном уровне обеспечивать рассмотрение запросов, заявлений и жалоб Субъектов, а также содействовать исполнению требований компетентных органов. Лица, виновные в нарушении требований настоящей политики, привлекаются к дисциплинарной ответственности.