Утверждаю
Директор ГБПОУ КТСТГХ
_____ Л.П. Самкова
Приказ от 15.04.2017 г. № 105

Рассмотрено
Советом Техникума
Протокол от 14.04. 2017 г. № 1_

Политика
в отношении обработки и защиты персональных данных
в Государственном бюджетном профессиональном образовательном учреждении «Курганский техникум строительных технологий городского хозяйства»

1. Основные положения

Настоящая Политика определяет порядок создания, обработки и защиты персональных данных сотрудников, обучающихся и выпускников Техникума.

Основанием для разработки Политики являются:

- Конституция РФ от 12 декабря 1993 г. (ст. 2, 17-24, 41);
- глава 14 (ст. 85-90) Трудового кодекса РФ;
- часть 1 и 2, часть 4 Гражданского кодекса РФ;
- Закон РФ от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации»;
- Федеральный закон от 02 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;
- Федеральный закон от 07 июля 2003 г. № 126-ФЗ «О связи»;
- Федеральный закон Российской Федерации от 02 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;
- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Указ Президента РФ от 06 марта 1997 г. № 188 (ред. от 23 сентября 2005 г.) «Об утверждении перечня сведений конфиденциального характера»;
- Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановление Правительства Российской Федерации от 21 марта 2012 г. № 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»;
- Постановление Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Регламентирующие документы ФСТЭК России и ФСБ России об обеспечении безопасности персональных данных:

- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (Выписка) (утв. ФСТЭК РФ 15 февраля 2008 г.);

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 информационная система персональных данных, создаваемых и эксплуатируемых в Техникуме.

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

1.3. Персональные данные являются конфиденциальной, охраняемой информацией и на них распространяются все требования, установленные внутренними документами образовательного учреждения к защите конфиденциальной информации.

1.4.Политика служит основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности ПДн образовательных учреждений, а также нормативных и методических документов, обеспечивающих ее реализацию.

1.5.Является общедоступным документом, декларирующим концептуальные основы деятельности оператора при обработке персональных данных.

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.
Техникум– Государственное бюджетное профессиональное образовательное учреждение «Курганский техникум строительных технологий и городского хозяйства».

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.

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

- реализации образовательных и воспитательных программ Техникума;
- проведения и(или) участия сотрудников, обучающихся Техникума в олимпиадах, семинарах, конкурсах, форумах, соревнованиях, состязаниях, смотрах, выставках;
- направление сотрудников на обучение;
- дистанционного обучения;
- проведения мониторинга образовательной деятельности;
- ведения финансово-хозяйственной деятельностью Техникума;

- социальной защиты сотрудников и обучающихся Техникума;

в иных случаях предусмотренных законодательством РФ.

4. Принципы обеспечения защиты информации, составляющей персональные данные

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

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

4.1. 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.

4.2. 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.

4.3. 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.

4.4. 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.

4.5. 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.

4.6. 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.

4.7. 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.

4.8. 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».

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

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

5.2. Защита 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 Техникума.

5.3. Регламентация доступа сотрудников Техникума к документам и базам данных с персональными сведениями входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий руководителями и сотрудниками Техникума. 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 запираемых помещениях, сейфах, шкафах;
- наличие необходимых условий в помещении для работы с документами и базами данных с персональными сведениями; в помещении, в котором находится вычислительная техника;
- ознакомление работников, непосредственно осуществляющих обработку ПДн, с требованиями законодательства РФ в сфере ПДн, локальными актами оператора в сфере ПДн.
- 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.

5.4. 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.

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

6. Доступ к персональным данным

6.1. Сотрудники Оператора, которые в силу выполняемых служебных (трудовых) обязанностей постоянно работают с ПДн, получают доступ к необходимым категориям ПДн на срок выполнения ими соответствующих должностных обязанностей на основании перечня лиц, допущенных к работе с ПДн, который утверждается директором Оператора.

6.2. Список лиц, имеющих доступ к ПДн для информационной системы, должен поддерживаться в актуальном состоянии.

6.3. Оператором установлен разрешительный порядок доступа к ПДн. Сотрудникам Оператора предоставляется доступ к работе с ПДн в пределах и объеме, необходимых для выполнения ими для выполнения служебных (трудовых) обязанностей.

6.4. Временный или разовый допуск к работе с ПДн в связи со служебной необходимостью может быть получен сотрудником Оператора по согласованию директора.

6.5. Доступ к ПДн третьих лиц, не являющихся сотрудниками Оператора без согласия субъекта ПДн, запрещен, за исключением доступа сотрудников органов исполнительной власти, осуществляемого в рамках мероприятий по контролю и надзору за исполнением законодательства, реализации функций и полномочий соответствующих органов государственной власти. Предоставление информации по запросу или требованию органа государственной власти осуществляется с разрешения директора.

6.6. В случае если сотруднику сторонней организации необходим доступ к ПДн Оператора, то необходимо, чтобы в договоре со сторонней организацией были прописаны условия конфиденциальности ПДн и обязанность сторонней организации и ее сотрудников по соблюдению требований текущего законодательства в области защиты ПДн. Кроме того, в случае доступа к ПДн лиц, не являющихся сотрудниками Оператора, должно быть получено согласие субъектов ПДн на предоставление их ПДн третьим лицам. Указанное согласие не требуется, если ПДн предоставляются в целях исполнения гражданско-правового договора, заключенного Оператором с субъектом ПД.

6.7. Доступ сотрудника Оператора к ПДн прекращается с даты, прекращения трудовых отношений, либо даты изменения должностных обязанностей сотрудника и/или исключения сотрудника из списка лиц, имеющих право доступа к ПДн. В случае увольнения все носители, содержащие ПДн, которые в соответствии с должностными обязанностями находились в распоряжении работника во время работы, должны быть переданы соответствующему должностному лицу.

7. Обработка персональных данных

7.1. При обработке персональных данных в образовательном учреждении соблюдаются конституционные права и свободы человека и гражданина на неприкосновенность частной жизни, личную и семейную тайну.

7.2. Образовательное учреждение не вправе обрабатывать персональные данные субъектов ПДн об их расовой, политических взглядах, религиозных или философских убеждениях, интимной жизни.

7.3. Категории субъектов персональных данных:

В техникуме обрабатываются ПД следующих субъектов ПД :

- физические лица, состоящие с Техникумом в трудовых отношениях;
- физические лица, уволившиеся из Техникума;
- физические лица, являющиеся кандидатами на работу;
- физические лица, состоящие с Техникумом в гражданско-правовых отношениях;
- физические лица, являющиеся абитуриентами, обучающимися, выпускниками Техникума (их законные представители).

7.4. Источники получения персональных данных:

- субъект ПДн;
- законный представитель субъекта.

7.5. При наличии законных оснований получателем персональных данных субъекта могут являться:

- Налоговые органы;
- Пенсионный Фонд РФ;
- Фонд социального страхования РФ;
- Федеральная служба государственной статистики РФ;
- Фонд обязательного медицинского страхования РФ;
- правоохранительные органы;
- Органы попечительства и опеки;
- банки и кредитные организации;
- и иные организации и учреждения.

7.6. Персональные данные субъектов в образовательном учреждении обрабатываются как на бумажных носителях, так и в электронном виде – в компьютерных программах и электронных базах данных (в ИСПДн) без передачи по незащищенным техническим каналам связи.

7.7. Обработка персональных данных по общему правилу происходит до утраты правовых оснований.

7.8. Срок хранения документов, содержащих персональные данные, определяется "Перечнем типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения", утвержденный Приказом Министерства культуры РФ от 25.08.2010 № 558 и в иных случаях, предусмотренных законодательством РФ.

7.9. Трансграничная передача персональных данных не осуществляется.

7.10. Сведениями, составляющими персональные данные, является любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

7.11. Персональные данные могут обрабатываться только в целях, непосредственно связанных с деятельностью Техникума, в частности для:

- осуществления образовательной и воспитательной программ Техникума;
- проведения и(или) участия сотрудников, обучающихся Техникума в олимпиадах, семинарах, конкурсах, форумах, соревнованиях, состязаниях, смотрах, выставках;
- направление сотрудников на обучение;
- направление работ сотрудников, обучающихся на конкурсы;

- дистанционного обучения;
- проведения мониторинга образовательной деятельности;
- ведения финансово-хозяйственной деятельностью Техникума;
- организации кадрового учета, ведение кадрового делопроизводства, содействие работникам в трудоустройстве, обучении и продвижении по службе, исполнение налогового законодательства РФ в связи с исчислением и уплатой НДФЛ, а также пенсионного законодательства РФ при формировании и представлении персонифицированных данных о каждом получателе доходов, учитываемых при начислении страховых взносов на обязательное пенсионное страхование и обеспечение, заполнение первичной статистической документации;
- заключение, исполнение и прекращение гражданско-правовых договоров;
- защиты жизни, здоровья или иных жизненно важных интересов субъектов персональных данных;
- социальной защиты сотрудников и студентов Техникума
- в иных случаях предусмотренных законодательством РФ.

8. Основные права субъекта ПД и обязанности оператора

8.1. Основные права субъекта ПД

Субъект имеет право на доступ к его персональным данным и следующим сведениям:

- подтверждение факта обработки ПД оператором;
- правовые основания и цели обработки ПД;
- цели и применяемые оператором способы обработки ПД;
- наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к ПД или которым могут быть раскрыты ПД на основании договора с оператором или на основании федерального закона;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом ПД прав, предусмотренных настоящим Федеральным законом;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПД по поручению оператора, если обработка поручена или будет поручена такому лицу;
- обращения к оператору и направлению ему запросов;
- обжалование действий или бездействия оператора.

8.2. Обязанности Оператора

Оператор обязан:

- при сборе ПД предоставить информацию об обработке ПД; - в случаях, если ПД были получены не от субъекта ПД, уведомить субъекта;
- при отказе в предоставлении ПД субъекту разъясняются последствия такого отказа;
- опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПД, к сведениям о реализуемых требованиях к защите ПД;
- принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПД от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования,

предоставления, распространения ПД а также от иных неправомерных действий в отношении ПД;

– давать ответы на запросы и обращения Субъектов ПД, их представителей и уполномоченного органа по защите прав субъектов ПД.

9.Порядок обеспечения защиты информации при эксплуатации ИСПДн

9.1. Эксплуатация ИСПДн должна осуществляться в полном соответствии с утвержденной проектной, организационно-распорядительной и эксплуатационной документацией ИСПДн.

9.2. Ответственность за обеспечение защиты информации в процессе эксплуатации ИСПДн возлагается на заместителя директора Техникума.

9.3. Ответственность за соблюдение установленных требований по защите информации при ее обработке в ИСПДн возлагается на непосредственных исполнителей ИСПДн (пользователей, администраторов, обслуживающий персонал).

9.4. За нарушение установленных требований по защите информации заместитель директора Техникума, в ведении которой находится ИСПДн, и (или) непосредственный исполнитель привлекаются к ответственности в соответствии с действующим в РФ законодательством.

10. Контроль состояния и эффективности защиты ИСПДн

10.1. В ИСПДн должен осуществляться контроль и (или) аудит соответствия обработки ПДн действующим в РФ законодательству и требованиям к защите ПДн, а так же настоящей Политике и локальным актам Техникума.

10.2. Контроль заключается в оценке выполнения требований нормативных документов, обоснованности принятых мер и оценке эффективности принятых мер по обеспечению ПДн.

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

10.4. В процессе эксплуатации ИСПДн в целях защиты информации от НСД осуществляются оперативный контроль и периодический контроль за выполнением исполнителями требований действующих нормативных документов по вопросам обеспечения безопасности и защиты ПДн.

10.5. С целью своевременного выявления и предотвращения утечки информации, исключения или существенного затруднения НСД и предотвращения специальных воздействий (программно-технических и др.), вызывающих нарушение целостности информации или работоспособность технических средств, в ИСПДн Техникума проводится плановый периодический (не реже одного раза в год) контроль состояния защиты информации.

10.6. При проведении плановых проверок осуществляется контроль ведения учетной документации, защищенности ИСПДн от утечки ПДн по техническим каналам, выборочный контроль содержимого накопителей и носителей информации, и т.п.

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

11.Ответственность за разглашение персональных данных и нарушение

11.1. Техникум ответственен за персональную информацию, которая находится в его распоряжении и закрепляет персональную ответственность

сотрудников за соблюдением, установленных в организации принципов уважения приватности.

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

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

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

11.5.Сотрудники Техникума 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.