МИНИСТЕРСТВО ОБРАЗОВАНИЯ КРАСНОЯРСКОГО КРАЯ
КРАЕВОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«Зеленогорский техникум промышленных технологий и сервиса»

ПРИКАЗ

«08» декабря 2017г. г. Зеленогорск № 603 од

Об утверждении Политики в отношении обработки персональных данных в краевом государственном бюджетном профессиональном образовательном учреждении «Зеленогорский техникум промышленных технологий и сервиса»

В целях соблюдения требований ч. 2 ст. 18.1 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» и в целях организации работ по обеспечению безопасности персональных данных

ПРИКАЗЫВАЮ:

1. Утвердить Политику в отношении обработки персональных данных в краевом государственном бюджетном профессиональном образовательном учреждении «Зеленогорский техникум промышленных технологий и сервиса» (Приложение № 1).
2. Специалистам по персоналу Поповой Е.В., Конон Е.Н. ознакомить работников с Политикой под роспись.
3. Заведующему отделением Л.Н. Тихоновой обеспечить размещение приказа на официальном сайте в течение десяти рабочих дней.
4. Контроль за исполнением приказа оставляю за собой.

Директор С.П. Родченко

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 0264A24C00A0AC7D9949BE6F4AF6D33EC8
Владелец: Родченко Сергей Петрович
Действителен: с 29.12.2020 до 29.03.2022

Приложение № 1

к приказу от

«8» декабря 2017 № 603 од

Политика в отношении обработки персональных данных в краевом государственном бюджетном профессиональном образовательном учреждении «Зеленогорский техникум промышленных технологий и сервиса»

1. Общие положения

1.1. Настоящая Политика в отношении обработки персональных данных (далее – Политика) в краевом государственном бюджетном профессиональном образовательном учреждении «Зеленогорский техникум промышленных технологий и сервиса» (далее – КГБПОУ «Зеленогорский техникум промышленных технологий и сервиса», техникум) определяет основные подходы к обработке и защите персональных данных (далее –ПДн) в КГБПОУ «Зеленогорский техникум промышленных технологий и сервиса» и содержит сведения о реализуемых требованиях в защите ПДн.

Политика представляет собой систематизированное изложение целей, задач, принципов и условий обработки ПДн и действует в отношении любой информации о субъекте ПДн (физическом лице), которую техникум вправе обрабатывать.

1.2. Настоящая Политика разработана в соответствии с:

- Конституцией Российской Федерации;
- Трудовым кодексом Российской Федерации;
- Федеральным законом от 27.06.2006 № 152-ФЗ «О персональных данных»;

- иными нормативно-правовыми актами, регулирующими отношения, связанные с обработкой и защитой ПДн;

- Уставом КГБПОУ «Зеленогорский техникум промышленных технологий и сервиса».

1.3. Политика является методологической основой для:

- принятия управленческих решений и разработки практических мер по воплощению политики в отношении обработки ПДн и их защиты и выработки комплекса согласованных правовых, организационных, технических и иных мер, направленных на выявление угроз в отношении ПДн и их ликвидацию в техникуме;

- координации деятельности структурных подразделений при проведении работ по созданию, развитию и эксплуатации информационных технологий с соблюдением требований по обеспечению безопасности информации, которые применяются при обработке ПДн;

- разработки предложений по совершенствованию правовых, организационных, технических и иных мер по обработке и защите ПДн в техникуме;

- построения комплексной системы обработки и защиты ПДн, в том числе при их обработке в информационных системах персональных данных (далее – ИСПДн) в техникуме должна способствовать оптимизации затрат на её построение.

1.4. Действие настоящей Политики распространяется на ПДн всех категорий субъектов ПДн, обработка которых осуществляется в техникуме, а именно:

- работников, состоящих в трудовых отношениях с техникумом;

- лиц, участвующих в конкурсе на зачисление в техникум;

- слушателей, обучающихся (далее – обучающиеся);

- членов ГИА, ГЭК, ГАК;

- исполнителей по гражданско-правовым договорам;

- посетителей техникума;

- физических лиц, пользующихся услугами техникума;

- физических лиц, вступающих в расчётно-финансовые отношения с техникумом;

- иных физических лиц, которые обращаются с запросами в техникум.

2. Цели и задачи политики. Принципы обработки ПДн в КГБПОУ «Зеленогорский техникум промышленных технологий и сервиса»

2.1. Основные цели Политики:

2.1.1. Повышение доверия к техникуму со стороны абитуриентов, обучающихся, работников КГБПОУ «Зеленогорский техникум промышленных технологий и сервиса».

2.1.2. Обеспечение режима конфиденциальности ПДн, защиты от несанкционированного распространения;

- повышение стабильности функционирования КГБПОУ «Зеленогорский техникум промышленных технологий и сервиса», обеспечение реализации уставных целей и осуществления направлений деятельности, указанных в Уставе КГБПОУ «Зеленогорский техникум промышленных технологий и сервиса».

2.1.3. Содействие субъектам ПДн в осуществлении учебной, трудовой и иной деятельности, обеспечение защиты прав и свобод субъектов ПДн КГБПОУ «Зеленогорский техникум промышленных технологий и сервиса» при обработке их ПДн, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

2.1.4. Регулирование отношений, связанных с обработкой ПДн субъектов ПДн, осуществляемой техникумом.

2.1.5. Определение задач, принципов, условий и порядка обработки ПДн субъектов ПДн в КГБПОУ «Зеленогорский техникум промышленных технологий и сервиса».

2.1.6. Установление ответственности должностных лиц КГБПОУ «Зеленогорский техникум промышленных технологий и сервиса» за невыполнение требований норм, регулирующих обработку и защиту ПДн.

2.2. Основные задачи Политики:

2.2.1. Определение направлений деятельности техникума по обработке и защите ПДн лиц, поступающих на обучение в техникум, обучающихся, работников КГБПОУ «Зеленогорский техникум промышленных технологий и сервиса» и иных лиц.

2.2.2. Установление оптимальных требований по обеспечению защиты ПДн при их обработке с использованием средств автоматизации и без использования средств автоматизации.

2.2.3. Повышение эффективности мероприятий обработки и защиты ПДн.

2.3. Принципы обработки ПДн:

2.3.1. Обработка ПДн в техникуме должна осуществляться в соответствии с действующим законодательством в сфере защиты ПДн, Уставом КГБПОУ «Зеленогорский техникум промышленных технологий и сервиса», настоящей Политикой и иными локальными нормативными актами КГБПОУ «Зеленогорский техникум промышленных технологий и сервиса».

2.3.2. Обработка ПДн должна ограничиваться достижением конкретных, заранее определённых и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн.

2.3.3. Не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.

2.3.4. Обработке подлежат только ПДн, которые отвечают целям обработки.

2.3.5. Содержание и объём обрабатываемых ПДн должны соответствовать заявленным целям обработки. Обрабатываемые ПДн не

должны быть избыточными по отношению к заявленным целям их обработки.

2.3.6. При обработке ПДн должны быть обеспечены точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн.

2.3.7. КГБПОУ «Зеленогорский техникум промышленных технологий и сервиса» должно принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

2.3.8. Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом и (или) договором, стороной которого либо выгодоприобретателем по которому является субъект ПДн.

2.3.9. Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

3. Условия и порядок обработки ПДн

3.1. Обработка ПДн в техникуме осуществляется с соблюдением принципов, определённых п. 2.3. настоящей Политики.

3.2. Обработка ПДн допускается в следующих случаях:

3.2.1. Обработка ПДн осуществляется с согласия субъекта ПДн на обработку его ПДн, за исключением случаев, определённых федеральными законами;

3.2.2. Обработка ПДн необходима для осуществления и выполнения функций, полномочий и обязанностей, возложенных на КГБПОУ «Зеленогорский техникум промышленных технологий и сервиса» законодательством Российской Федерации, Уставом КГБПОУ

«Зеленогорский техникум промышленных технологий и сервиса» и (или) договором;

3.2.3. Обработка ПДн необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;

3.2.4. Обработка ПДн необходима для исполнения договора, стороной которого либо выгодоприобретателем по которому является субъект ПДн, а также для заключения договора по инициативе субъекта ПДн или договора, по которому субъект ПДн будет являться выгодоприобретателем;

3.2.5. Обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн, если получение согласия субъекта ПДн невозможно;

3.2.6. Обработка ПДн необходима для осуществления прав и законных интересов техникума или третьих лиц, либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта ПДн;

3.2.7. Обработка ПДн осуществляется в статистических или иных целях, за исключением целей, указанных в статье 15 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», при условии обязательного обезличивания ПДн;

3.2.8. Осуществляется обработка ПДн, доступ неограниченного круга лиц к которым предоставлен субъектом ПДн, либо по его просьбе;

3.2.9. Осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральными законами.

3.3. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни в техникуме не производится.

3.4. Обработка персональных данных о судимости в техникуме осуществляется в соответствии с законодательством Российской Федерации.

3.5. Обработка биометрических ПДн в техникуме осуществляется в учётом требований, установленных ст. ст. 10, 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

3.6. КГБПОУ «Зеленогорский техникум промышленных технологий и сервиса» вправе поручить обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено федеральным законом, на основании заключённого с этим лицом договора.

3.7. Техникум осуществляет обработку ПДн с использованием средств автоматизации и без использования средств автоматизации.

4. Основные принципы построения системы безопасности ПДн

4.1. Основными принципами являются:

ЗАКОННОСТЬ – осуществление защитных мероприятий и разработка системы безопасности ПДн КГБПОУ «Зеленогорский техникум промышленных технологий и сервиса» в соответствии с действующим законодательством в области защиты ПДн, а также других законодательных актов по безопасности информации Российской Федерации, с применением всех дозволенных методов обнаружения и пресечения правонарушений при работе с ПДн. Принятые меры безопасности ПДн не должны препятствовать доступу правоохранительных органов в предусмотренных законодательством случаях. Все пользователи ИСПДн КГБПОУ «Зеленогорский техникум промышленных технологий и сервиса» должны иметь представление об ответственности за правонарушения в области обработки ПДн.

СИСТЕМНОСТЬ – учёт всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения

безопасности ПДн. При создании системы защиты должны учитываться все слабые и наиболее уязвимые места ИСПДн техникума, а также характер, возможные объекты и направления атак на неё со стороны нарушителей. Система защиты должна строиться с учётом не только всех известных каналов проникновения и несанкционированного доступа к информации, но и с учётом возможности появления принципиально новых путей реализации угроз безопасности.

КОМПЛЕКСНОСТЬ – использование методов и средств защиты компьютерных систем, согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все значимые каналы реализации угроз и не содержащей слабых мест на стыках отдельных её компонентов. Защита должна строиться эшелонировано. Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами.

НЕПРЕРЫВНОСТЬ ЗАЩИТЫ - постоянная административная поддержка (своевременная смена и обеспечение правильного хранения и применения имён, паролей и т.д.).

СВОЕВРЕМЕННОСТЬ – носит упреждающий характер мер обеспечения безопасности ПДн, т.е. постановку задач по комплексной защите ПДн и реализацию мер обеспечения безопасности ПДн на ранних стадиях разработки ИСПДн в целом и их систем защиты в частности. Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой ИСПДн, что позволяет учитывать требования безопасности при проектировании архитектуры и создаёт более эффективные (по затратам ресурсов, стойкости) системы, обладающие достаточным уровнем защищённости.

ПРЕЕМСТВЕННОСТЬ И СОВЕРШЕНСТВОВАНИЕ – постоянное совершенствование мер и средств защиты ПДн на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования ИСПДн техникума и системы её

защиты с учётом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

РАЗУМНАЯ ДОСТАТОЧНОСТЬ – соответствие уровня затрат на обеспечение безопасности ПДн ценности информационных ресурсов и величине возможного ущерба от разглашения, утраты, утечки, уничтожения и искажения. Используемые меры и средства обеспечения безопасности информационных ресурсов не должны заметно ухудшать эргономические показатели работы компонентов ИСПДн техникума. Излишние меры безопасности не должны приводить в экономической неэффективности, снижению эффективности работы персонала.

ПЕРСОНАЛЬНАЯ ОТВЕТСТВЕННОСТЬ – возложение ответственности за обеспечение безопасности ПДн и системы их обработки на каждого работника в пределах его должностных обязанностей. Распределение прав и обязанностей работников строится таким образом, чтобы в случае любого нарушения круг виновников был чётко известен или сведён к минимуму.

МИНИМИЗАЦИЯ ПОЛНОМОЧИЙ – предоставление пользователям минимальных прав доступа в соответствии со служебной необходимостью. Доступ к ПДн должен предоставляться только в том случае и объёме, если это необходимо сотруднику для выполнения его должностных обязанностей.

ИСКЛЮЧЕНИЕ КОНФЛИКТА ИНТЕРЕСОВ – чёткое разделение обязанностей работников и исключение ситуаций, когда сфера ответственности работников допускает конфликт интересов. Сферы потенциальных конфликтов должны выявляться, минимизироваться и находиться под строгим независимым контролем.

ГИБКОСТЬ СИСТЕМЫ ЗАЩИТЫ - способность реагировать на изменения внешней среды и условий осуществления техникумом своей деятельности. В число таких изменений входят:

- изменение организационной и штатной структуры;

- изменение существующих или внедрение принципиально новых ИСПДн;

- новые технические средства и технологии.

ОТКРЫТОСТЬ АЛГОРИТМОВ И МЕХАНИЗМОВ ЗАЩИТЫ – обеспечение защиты не только за счёт секретности структурной организации и алгоритмов функционирования её подсистем. Знание алгоритмов работы системы защиты не должно давать возможности её преодоления. Это не означает, что информация об используемых системах и механизмах защиты должна быть общедоступна.

ПРОСТОТА ПРИМЕНЕНИЯ СРЕДСТВ ЗАЩИТЫ – механизмы и методы защиты должны быть понятны и просты в использовании. Применение средств и методов защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций.

ОБОСНОВАННОСТЬ И ТЕХНИЧЕСКАЯ РЕАЛИЗУЕМОСТЬ – реализация информационных технологий, технических, программных средств, средств и мер защиты ПДн на современном уровне развития науки и техники, обоснованные с точки зрения достижения заданного уровня безопасности информации и экономической целесообразности, соответствующие установленным нормам и требованиям по безопасности ПДн.

СПЕЦИАЛИЗАЦИЯ И ПРОФЕССИОНАЛИЗМ – реализация административных мер и эксплуатация средств защиты осуществляемая профессионально подготовленными специалистами техникума (ответственными за организацию обработки и защиты ПДн).

ОБЯЗАТЕЛЬНОСТЬ КОНТРОЛЯ – своевременность и обязательность выявления и пресечения попыток нарушения

установленных правил, обеспечения безопасности ПДн на основе используемых систем и средств защиты ПДн, при совершенствовании критериев и методов оценки эффективности этих систем и средств. Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

5. Меры и методы обеспечения требуемого уровня защиты информационных ресурсов

5.1. При обработке ПДн в техникуме должны приниматься необходимые правовые, организационные и технические меры для их защиты от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения и от иных неправомерных действий в отношении них.

5.2. Обеспечение безопасности ПДн должно достигаться:

- назначением ответственных лиц за организацию обработки и обеспечение безопасности ПДн;
- полнотой, реальной выполнимостью и непротиворечивостью требований организационно-распорядительных документов КГБПОУ «Зеленогорский техникум промышленных технологий и сервиса»;
- подготовкой должностных лиц, ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности ПДн и процессов их обработки;
- персональной ответственностью за свои действия каждого работника, в рамках своих должностных обязанностей, имеющего доступ к информационным ресурсам техникума;
- осуществлением внутреннего контроля (аудита) соответствия обработки ПДн в техникуме Федеральному закону от 27.07.2006 № 152-

ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПДн, локальным актам КГБПОУ «Зеленогорский техникум промышленных технологий и сервиса» не реже одного раза в три года;

- ознакомлением лиц, поступающих на обучение, обучающихся, работников техникума, непосредственно осуществляющих обработку ПДн с положениями законодательства Российской Федерации о ПДн, в том числе с требованиями к защите ПДн, локальными актами КГБПОУ «Зеленогорский техникум промышленных технологий и сервиса» в отношении обработки ПДн и (или) обучением указанных работников;

- оценкой эффективности принимаемых мер по обеспечению безопасности ПДн;

- выявлением фактов несанкционированного доступа к персональным данным и принятием соответствующих мер по их защите;

- восстановлением ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

5.3. При обработке ПДн в ИСПДн необходимый уровень защиты должен достигаться:

5.3.1. Строгим учётом всех подлежащих защите ресурсов ИСПДн техникума (задач, информации, документов, серверов, каналов связи).

5.3.2. Наделением каждого работника (пользователя) минимально необходимыми для выполнения им своих должностных обязанностей полномочиями по доступу к информационным ресурсам техникума.

5.3.3. Чётким знанием и строгим соблюдением всеми пользователями ИСПДн техникума требований организационно-распорядительных документов по вопросам обеспечения безопасности информации.

5.3.4. Определением угроз безопасности ПДн при их обработке в ИСПДн.

5.3.5. Непрерывным поддержанием необходимого уровня защищённости элементов информационной среды техникума.

5.3.6. Применением физических и технических средств защиты ресурсов системы и непрерывной административной поддержкой их использования.

6. Средства обеспечения безопасности ПДн

6.1. На технические средства защиты возлагается решение следующих основных задач:

- идентификация и аутентификация пользователей при помощи имён или специальных аппаратных средств;

- регламентация и управление доступом пользователей в помещения, к физическим и логическим устройствам;

- защита от проникновения компьютерных вирусов и разрушительного воздействия вредоносных программ;

- защита данных системы защиты на файловом сервере от доступа пользователей, в чьи должностные обязанности не входит работа с информацией, находящейся на нём.

6.2. В состав системы защиты должны быть включены следующие технические средства защиты:

- средства разграничения доступа к данным;

- средства регистрации доступа к компонентам ИСПДн и контроля за использованием информации;

- средства реагирования на нарушения режима информационной безопасности.

6.3. Технические средства разграничения доступа должны по возможности быть составной частью единой системы контроля доступа на контролируемую территорию, в отдельные помещения, к компонентам информационной среды техникума и элементам защиты ПДн (физический доступ), к информационным ресурсам (документам, носителям информации, файлам, справкам, архивам и т.п.), к активным ресурсам (прикладным ресурсам и т.п.), к операционной системе, системным программам и программам защиты.

6.4. Средства обеспечения целостности должны включать средства резервного копирования, программы антивирусной защиты, программы восстановления целостности операционной среды и базы данных.

6.5. Средства оперативного контроля должны обеспечивать обнаружение и регистрацию всех событий (действий пользователей, попыток несанкционированного доступа и т.д.), которые могут повлечь за собой нарушение безопасности и привести к возникновению кризисных ситуаций.

6.6. Для своевременного выявления и предотвращения утечки ПДн за счёт несанкционированного доступа, а также предупреждения возможных специальных воздействий, направленных на уничтожение ПДн, разрушение средств информатизации должен осуществляться контроль эффективности защиты ПДн, оценка эффективности мер защиты ПДн с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

7. Ответственность за нарушения в области обработки и защиты ПДн

7.1. Обязанности работников техникума, осуществляющих обработку и защиту ПДн, а также их ответственность, определяются должностными инструкциями, иными локальными нормативными, распорядительными актами КГБПОУ «Зеленогорский техникум промышленных технологий и сервиса».

8. Утверждение, введение в действие, изменение Политики

8.1. Настоящая Политика утверждается приказом директора КГБПОУ «Зеленогорский техникум промышленных технологий и сервиса».

8.2. Техникум имеет право вносить изменения в настоящую Политику:

- по мере принятия новых нормативных правовых актов в сфере ПДн или внесения в них изменений;

- по мере принятия локальных нормативных актов техникума, регламентирующих организацию обработки и обеспечение безопасности ПДн.

9. Ознакомление с Политикой

9.1. Все заинтересованные лица могут ознакомиться с настоящей Политикой в отделе кадров, а также на официальном сайте техникума.

10. Хранение и рассылка экземпляров Политики

10.1. Контрольный экземпляр настоящей Политикой хранится в отделе кадров.

Электронная копия настоящей Политики размещена на сайте техникума для обеспечения неограниченного доступа.