МИНИСТЕРСТВО ОБРАЗОВАНИЯ МОСКОВСКОЙ ОБЛАСТИ
ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ МОСКОВСКОЙ ОБЛАСТИ «МЕЖРЕГИОНАЛЬНЫЙ ЦЕНТР КОМПЕТЕНЦИЙ — ТЕХНИКУМ ИМЕНИ С.П. КОРОЛЕВА»
(ГАПОУ МО «МЦК — Техникум имени С.П. Королева)

Адрес: 141068, Московская область, город Королев, мкр. Текстильщик, улица Молодежная, дом № 7.
Контактные координаты: телефон/факс приемной директора 515-41-43, бухгалтерии 516-64- 71.

УТВЕРЖДАЮ
Директор _____ И.А. Ласкина
«14» ___06___ 2025 г.

ИНСТРУКЦИЯ

РАБОТНИКА СТРУКТУРНОГО ПОДРАЗДЕЛЕНИЯ, ОСУЩЕСТВЛЯЮЩЕГО ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ В ПОДРАЗДЕЛЕНИЯХ ГАПОУ МО «МЦК — ТЕХНИКУМ ИМЕНИ С.П. КОРОЛЕВА»

г. Королев, 2025

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Настоящая Инструкция работника структурного подразделения, осуществляющего обработку персональных данных в подразделениях ГАПОУ МО «МЦК — Техникум имени С.П. Королева» (далее – Работник), разработана на основании требований Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных», в соответствии с требованиями локальных нормативных актов государственного автономного профессионального образовательного учреждения Московской области «Межрегиональный центр компетенций — Техникум имени С.П. Королева» (далее – Техникум).

1.2 Работник – лицо, непосредственно занимающееся получением, обработкой, хранением, учетом персональных данных (далее – ПДн).

1.3 Работник допускается к работе после изучения положений и инструкций по правилам обработки ПДн и прохождения инструктажа.

1.4 Работник в процессе осуществления своих обязанностей по обработке ПДн руководствуется законодательством Российской Федерации и иными нормативными правовыми актами в области обеспечения безопасности ПДн, локальными нормативными актами Техникума.

1.5 Работа с ПДн строится на следующих принципах:

Принцип персональной ответственности – за каждый документ (независимо от типа носителя: бумажный, электронный) персональную ответственность несет конкретный работник.

Принцип контроля и учета – все операции с документами должны отражаться в соответствующих журналах и карточках (передача из рук в руки, снятие копии и т.п.).

2 ОСНОВНЫЕ ОБЯЗАННОСТИ

2.1 Знать и выполнять требования локальных нормативных актов Техникума, затрагивающих вопросы защиты информации и обработки ПДн в подразделении.

2.2 Строго соблюдать установленные правила обеспечения защиты информации и обработки ПДн при работе с программными и техническими средствами автоматизированных информационных систем.

2.3 Соблюдать требования по защите информации и ПДн, правила работы со съемными машинными носителями информации, обеспечивать организационные меры по защите информации и ПДн.

2.4 Взаимодействовать с работниками, ответственными за защиту информации, по вопросам, связанным с выполнением требований по обработке ПДн.

2.5 Соблюдать требования по учету, хранению и использованию электронных и материальных носителей информации, предназначенных для хранения ПДн.

2.6 Знать перечень установленных в подразделении технических средств, входящих в состав информационных систем, и перечень задач, решаемых с их использованием.

2.7 Соблюдать утвержденный порядок проведения работ по установке, модернизации и устранению неисправностей аппаратных и программных средств компьютеров и серверов из состава информационных систем.

2.8 Ежедневно контролировать целостность печатей и пломб на допущенных к обработке персональных данных защищенных устройствах, компьютерах и серверах подразделения.

2.9 Соблюдать порядок использования и обеспечения сохранности персональных устройств идентификации пользователей.

2.10 Немедленно поставить в известность руководителя и ответственного за обеспечение безопасности ПДн своего подразделения в случаях:

несанкционированного доступа или разрушения целостности ПДн;

утери устройства личной идентификации;

при подозрении в компрометации личных ключей и паролей;

при обнаружении изменений в размещении средств вычислительной техники, нарушении целостности пломб (наклеек, нарушении или несоответствии номеров печати);

несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств;

отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию ПЭВМ, выхода из строя или неустойчивого функционирования узлов ПЭВМ или периферийных устройств (дисководов, принтера и т.п.);

некорректного функционирования установленных на ПЭВМ технических средств защиты;

непредусмотренных на ПЭВМ отводов кабелей и подключенных устройств.

2.11 Работникам запрещается:

использовать компоненты средств вычислительной техники автоматизированных систем в неслужебных целях;

самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ПЭВМ или устанавливать дополнительно любые программные и аппаратные средства;

осуществлять обработку ПДн в присутствии посторонних (не допущенных к данной информации) лиц;

оставлять в помещении посторонних лиц одних без присмотра;

записывать и хранить ПДн на неучтенных носителях информации;

записывать и хранить пароли, ключи доступа на видном месте;

оставлять включенной без присмотра на любое время автоматизированную систему, не активировав средства защиты от несанкционированного доступа;

передавать кому-либо свой личный идентификатор, кроме ответственного лица за обеспечение безопасности ПДн;

использовать личные идентификаторы для формирования цифровой подписи любых электронных документов, кроме как регламентированных технологическим процессом на рабочем месте;

оставлять без личного присмотра на рабочем месте или где бы то ни было свои личный идентификатор, машинные носители и распечатки, содержащие ПДн.

3 ПРАВА И ПОЛНОМОЧИЯ

3.1 Обращаться за помощью и консультациями к работникам, ответственным за защиту информации.

3.2 Участвовать в разработке мероприятий по совершенствованию защиты информации и обработки ПДн.

3.3 Обращаться к руководителю подразделения или ответственному за обеспечение защиты ПДн в подразделении с предложением о приостановке процесса обработки ПДн в случаях нарушения установленной технологии обработки или требований по защите информации и ПДн.

3.4 Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты информации и обработки ПДн, несанкционированного доступа, утраты, порчи защищаемых ПДн и технических средств из состава информационных систем.

3.5 Подавать свои предложения по совершенствованию организационных, технологических и технических мер защиты информации и обработки ПДн в подразделении.

4 ОТВЕТСТВЕННОСТЬ

4.1 Работник несет персональную ответственность за полноту и своевременное выполнение требований федеральных законов, нормативных документов в области защиты информации и обработки ПДн, а также настоящей Инструкции.

4.2 Работник, виновный в нарушении норм, регулирующих получение, обработку, защиту и передачу посторонним лицам ПДн, привлекается к дисциплинарной ответственности в порядке, установленном Трудовым кодексом Российской Федерации, локальными нормативными актами Техникума, а также к административной или уголовной ответственности в порядке, установленном законодательством Российской Федерации.