Утверждаю
Директор ЧПОУ «ММК»
_____Т.А.Зарубина
Приказ №_____от_____

# ИНСТРУКЦИЯ
## о порядке обеспечения конфиденциальности в ЧПОУ «ММК» при обращении с информацией, содержащей персональные данные

### 1. Общие положения

**1.1.** Предметом настоящей Инструкции являются обязательные для всех структурных подразделений и работников колледжа требования по обеспечению конфиденциальности документов, содержащих персональные данные.

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

**1.3.** Обеспечение конфиденциальности персональных данных не требуется в случае обезличивания персональных данных или в отношении общедоступных персональных данных. В общедоступные источники персональных данных (в том числе справочники, адресные книги) в целях информационного обеспечения с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, телефонный номер, сведения о профессии и иные персональные данные, предоставленные субъектом персональных данных.

**1.4.** Конфиденциальность персональных данных предусматривает обязательное согласие субъекта персональных данных (его законного представителя) или наличие иного законного основания на их обработку. Согласие субъекта персональных данных (его законного представителя) не требуется на обработку ПДн:

- в целях исполнения обращения, запроса субъекта персональных данных, трудового или иного договора с ним;
- адресных данных, необходимых для доставки почтовых отправлений организациями почтовой связи;
- данных, включающих в себя только фамилии, имена и отчества;
- в целях однократного пропуска на территорию, или в иных аналогичных целях.

**1.5.** В колледже формируются и ведутся перечни конфиденциальных данных (персональных данных), утверждённые директором колледжа. Осуществлять обработку и хранение конфиденциальных данных (персональных данных), не внесённых в перечень, запрещается.

**1.6.** Основные требования и мероприятия по обеспечению безопасности при обработке и хранении персональных данных установлены постановлениями Правительства Российской Федерации от 01 ноября 2012 года №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации». Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из неё.

**1.7.** Запрещается оставлять материальные носители с персональными данными без присмотра в незапертом помещении. Все сотрудники, постоянно работающие в помещениях, в которых ведётся обработка персональных данных, должны быть допущены к работе с соответствующими видами персональных данных.

Сотрудникам, работающим с персональными данными, запрещается сообщать их устно или письменно кому бы то ни было, если это не вызвано служебной необходимостью.

После подготовки и передачи документа в соответствии с резолюцией, файлы черновиков и вариантов документа переносятся подготовившим их сотрудником на маркированные носители, предназначенные для хранения персональных данных. Без согласования с руководителем структурного подразделения формирование и хранение баз данных (картотек, файловых архивов и др.), содержащих конфиденциальные данные, запрещается.

Передача персональных данных допускается только в случаях, установленных Федеральными законами Российской Федерации «О персональных данных», «О порядке рассмотрения обращений граждан Российской Федерации», действующими инструкциями по работе со служебными документами и обращениями граждан, а также по письменному поручению (резолюции) вышестоящих должностных лиц.

Запрещается передача персональных данных по телефону, факсу, электронной почте за исключением случаев, установленных законодательством и действующими инструкциями по работе со служебными документами и обращениями граждан. Ответы на запросы граждан и организаций даются в том объёме, который позволяет не разглашать в ответах конфиденциальные данные (персональные данные), за исключением данных, содержащихся в материалах заявителя или опубликованных в общедоступных источниках.

**1.8.** Работники колледжа, осуществляющие обработку или хранение конфиденциальных данных (персональных данных) в колледже, несут ответственность за обеспечение их информационной безопасности. Лица, виновные в нарушении норм, регулирующих обработку и хранение конфиденциальных данных (персональных данных), несут дисциплинарную, административную или уголовную ответственность в соответствии с действующим законодательством и ведомственными нормативными актами.

**1.9.** Работники подразделений колледжа и лица, выполняющие работы по договорам и контрактам, имеющие отношение к работе с конфиденциальной информацией (персональными данными), должны быть в обязательном порядке ознакомлены под расписку с настоящей Инструкцией.

## 2. Порядок обеспечения безопасности при обработке и хранении конфиденциальной информации (персональных данных), осуществляемой без использования средств автоматизации

**2.1.** Обработка конфиденциальной информации (персональных данных), осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных.

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки.

Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, исключающей одновременное копирование иных персональных данных, не подлежащих распространению и использованию.

**2.2.** При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:
**2.2.1** типовая форма или связанные с ней документы (инструкция по её заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, наименование и адрес Оператора (колледжа), фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых Оператором (колледжем) способов обработки персональных данных;
**2.2.2** типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных;
**2.2.3** типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;
**2.2.4** типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.
**2.3.** При ведении журналов, содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию, на которой находится Оператор (колледж), или в иных аналогичных целях, должны соблюдаться следующие условия:
**2.3.1** необходимость ведения такого журнала должна быть предусмотрена актом Оператора (колледжа), содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала, сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных на территорию, на которой находится Оператор (колледж), без подтверждения подлинности персональных данных, сообщённых субъектом персональных данных;
**2.3.2** копирование содержащейся в таких журналах информации не допускается;
**2.3.3** персональные данные каждого субъекта персональных данных могут заноситься в такой журнал не более одного раза в каждом случае пропуска субъекта персональных данных на территорию, на которой находится Оператор (колледж).
**2.4.** Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путём обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путём фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путём изготовления нового материального носителя с уточнёнными персональными данными.

### 3. Порядок обеспечения безопасности при обработке и хранении конфиденциальной информации (персональных данных), осуществляемой с использованием средств автоматизации

**3.1.** Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей

организационные меры и средства защиты информации, а также используемые в информационной системе информационные технологии.

Допуск лиц к обработке персональных данных в информационной системе осуществляется на основании соответствующих разрешительных документов и ключей (паролей) доступа.

Размещение информационных систем, специальное оборудование и организация работы с персональными данными должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого пребывания в этих помещениях посторонних лиц.

Компьютеры и (или) электронные папки, в которых содержатся файлы с персональными данными, для каждого пользователя должны быть защищены индивидуальными паролями доступа, состоящими из шести и более символов. Работа на компьютерах с персональными данными без паролей доступа, или под чужими или общими (одинаковыми) паролями, запрещается.

Пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в том числе Интернет, запрещается.

**3.2.** Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации. Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия.

**3.3.** При обработке персональных данных в информационной системе пользователями должно быть обеспечено:

**3.3.1** использование предназначенных для этого разделов (каталогов) носителей информации, встроенных в технические средства, или съёмных маркированных носителей;

**3.3.2** недопущение физического воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

**3.3.3** постоянное использование антивирусного обеспечения для обнаружения зараженных файлов и незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

**3.3.4** недопущение несанкционированных выноса из помещений, установки, подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.

**3.4.** При обработке персональных данных в информационной системе администратором системы должны обеспечиваться:

**3.4.1** обучение лиц, использующих средства защиты информации, применяемые в информационной системе, правилам работы с ними;

**3.4.2** учёт лиц, допущенных к работе с персональными данными в информационной системе, прав и паролей доступа;

**3.4.3** учёт применяемых средств защиты информации, эксплуатационной и технической документации к ним;

**3.4.4** контроль соблюдения условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

**3.4.5** описание системы защиты персональных данных.

**3.5.** Специфические требования по защите персональных данных в отдельных автоматизированных системах устанавливаются инструкциями по их использованию и эксплуатации.