Профессиональное образовательное частное учреждение

«КОЛЛЕДЖ ИНФОРМАТИКИ И ДИЗАЙНА»

(ПОЧУ «КИД»)

СОГЛАСОВАНО
Протокол заседания
Совета колледжа
от 23 августа 2022 г. № 5

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 3EDE720020AE5D8949F2A9A30F59C7F2
Владелец: ПЕНЬКО ОЛЬГА ВЛАДИМИРОВНА
Действителен: с 17.01.2022 до 17.04.2023

УТВЕРЖДАЮ
Директор
ПОЧУ «КИД»
_____ О.В. Пенько
25 августа 2022 г.

ПОЛОЖЕНИЕ

по сбору, обработке и защите персональных данных работников и обучающихся в Профессиональном образовательном частном учреждении «Колледж информатики и дизайна»

Москва – 2022

СОДЕРЖАНИЕ

1. Общие положения

1.1. Настоящее Положение предназначено для организации в колледже процесса обеспечения безопасности персональных данных согласно требованиям действующего федерального законодательства.

1.2. Положение вводится в действие с момента утверждения. Требования данного документа являются обязательными для всех работников колледжа, входящих в область распространения СМК.

1.3. Настоящее Положение разработано с учетом требований следующих правовых документов:

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 (с учетом поправок);
2. Трудовой кодекс Российской Федерации от 30 декабря 2001 г. N 197-ФЗ (с учетом поправок и изменений);
3. Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных» (с учетом поправок и изменений);
4. Федеральный закон от 27.07.2006 №149-ФЗ (ред. от 29.07.2017) «Об информации, информационных технологиях и о защите информации» (с изменений и дополнений);
5. Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных»;
6. Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
7. Устав Профессионального образовательного частного учреждения и локальные нормативные акты Профессионального образовательного частного учреждения «Колледж информатики и дизайна».

1.4. В настоящем Положении применяются следующие сокращения:

Колледж – Профессиональное образовательное частное учреждение «Колледж информатики и дизайна»;

Ответственный за ООПД – ответственный за организацию обработки персональных данных;

ОБПД – обеспечение безопасности персональных данных;

Ответственный за ОБПД – ответственный за обеспечение безопасности персональных данных;

ПД – персональные данные;

Положение – Положение по сбору, обработке и защите персональных данных работников и обучающихся в ПОЧУ «КИД».

1.5. Действие настоящего Положения распространяется на все процессы по сбору, систематизации, накоплению, хранению, уточнению, использованию,

распространению (в том числе передаче), обезличиванию, блокированию, уничтожению ПД, осуществляемые с использованием средств автоматизации и без их использования.

2. Роли персонала

2.1 Во исполнение положений настоящего документа и соответствия требованиям законодательства Российской Федерации о ПД в колледже введены следующие роли персонала:

- ответственный за организацию обработки персональных данных;
- ответственный за обеспечение безопасности персональных данных.

2.2 Назначение работников на роли Ответственного за организацию обработки персональных данных, Ответственного за обеспечение безопасности персональных данных осуществляется приказом директора колледже.

3. Обязательные мероприятия по обеспечению безопасности информационных систем персональных данных

3.1. Общие требования

3.1.1. В колледже до начала проведения работ по обеспечению безопасности ПД должна быть проведена инвентаризация информационных систем ПД путем опроса владельцев информационных систем на предмет наличия обработки в них ПД.

3.1.2. После инвентаризации информационных систем выявляются информационные системы ПД, в которых осуществляется автоматизированная обработка ПД, и информационные системы ПД, в которых осуществляется неавтоматизированная обработка ПД.

3.1.3. Для всех эксплуатируемых информационных систем ПД с автоматизированной обработкой ПД должны быть определены уровни защищенности ПД в соответствии с Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных».

3.1.4. В случае расширения состава данных в существующих информационных системах ПД, модернизации информационных систем ПД определение уровня защищенности ПД проводится в следующей последовательности:

1) на этапе эксплуатации (для ранее введенных в эксплуатацию и (или) модернизируемых информационных систем) приказом директора в колледже создается Комиссия по проведению определения уровней защищенности ПД в информационных системах ПД;

2) Комиссия в определенный приказом срок устанавливает категории, принадлежность и объем обрабатываемых ПД в информационных системах ПД, а также определяет тип актуальных для информационных систем ПД угроз безопасности ПД, связанных с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении;

3) Комиссия формирует акты определения уровней защищенности ПД для каждой информационной системы ПД, в которых указываются типы угроз безопасности ПД в информационных системах ПД, перечень обрабатываемых категорий ПД, их принадлежность и количество записей, содержащих ПД.

3.1.5. В колледже должны быть разработаны модели угроз безопасности ПД для всех информационных систем ПД. Модель угроз разрабатывается на основе методических документов, утвержденных в соответствии с ч. 5 ст. 19 Закона о персональных данных.

3.1.6. Выбор и реализация методов и способов защиты информации в информационных системах ПД осуществляются на основе Модели угроз и в зависимости от уровня защищенности ПД в информационных системах ПД.

3.1.7. Выбранные и реализованные методы и способы защиты ПД в информационных системах ПД должны обеспечивать нейтрализацию выявленных угроз безопасности ПД при их обработке в информационных системах ПД в составе системы защиты ПД.

3.1.8. Для проведения работ по выбору и реализации методов и способов защиты ПД (включая техническое проектирование системы защиты ПД, внедрение средств защиты ПД, сопровождение средств защиты ПД и т. д.) могут привлекаться подрядные организации, имеющие лицензию на осуществление деятельности по технической защите конфиденциальной информации.

3.1.9. Общие технические требования по защите ПД в информационных системах ПД колледже приведены в разделе 4.

4. Обеспечение технической защиты персональных данных

4.1. Общие требования

4.1.1. ОБПД при их обработке в информационных системах ПД должно осуществляться на всех стадиях жизненного цикла информационных систем ПД и состоять из согласованных мероприятий, направленных на предотвращение (нейтрализацию) и устранение угроз безопасности ПД в информационных системах ПД, минимизацию возможного ущерба, а также мероприятий по восстановлению данных и нормального функционирования информационных систем ПД в случае реализации угроз.

4.1.2. В целях защиты ПД от несанкционированного доступа и иных неправомерных действий мероприятия по организации и техническому

обеспечению безопасности ПД для каждой информационной системы ПД должны включать:

1) определение уровней защищенности ПД в информационной системе ПД на основании Требований к защите ПД при их обработке в информационных системах ПД, утвержденных постановлением Правительства Российской Федерации от 01.11.2012 № 1119;

2) выявление и закрытие технических каналов утечки ПД на основе анализа и актуализации Модели угроз безопасности ПД;

3) выбор и реализацию организационных и технических методов и способов защиты информации в информационной системе в зависимости от уровня защищенности ПД в информационной системе ПД с учетом особенностей инфраструктуры и с учетом актуальных угроз безопасности ПД в информационной системе ПД;

4) установку, настройку и применение соответствующих программных, аппаратных и программно-аппаратных средств защиты информации;

5) разработку дополнений к трудовым договорам (или функциональным инструкциям) по обеспечению безопасности ПД при их обработке в информационной системе ПД для персонала, задействованного в эксплуатации данной информационной системе ПД (подразделы А.1 и А.2 Приложения А).

4.1.3. Предотвращение утечки ПД по техническим каналам за счет побочных электромагнитных излучений и наводок, а также за счет электроакустических преобразований реализуется в колледже организационными мерами и не требует специальных технических решений.

4.1.4. Защита ПД при их обработке в информационной системе ПД от несанкционированного доступа и иных неправомерных действий должна осуществляться в колледже следующими методами и способами:

– реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам (включая ПД), информационной системе, содержащей ПД и связанные с ее работой документами;
– ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку ПД, а также хранятся носители информации, содержащие ПД;
– разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам (включая ПД), программным средствам обработки (передачи) и защиты ПД;
– регистрация действий пользователей и обслуживающего персонала информационной системы ПД, мониторинг попыток несанкционированного доступа;
– учет и хранение съемных носителей информации с ПД и их обращение, исключающее хищение, подмену и уничтожение;

– использование защищенных каналов связи, используемых для передачи ПД;

– размещение технических средств, позволяющих осуществлять обработку ПД в пределах контролируемой территории;

– предотвращение внедрения в информационную систему ПД вредоносных программ (программ вирусов) и программных закладок;

– регистрация событий и мониторинг процессов обработки информации;

– контроль целостности программных средств;

– регистрация запуска (остановки) программ обработки ПД;

– регистрация вывода ПД на печать.

4.1.5. При организации взаимодействия информационной системы ПД с информационно телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования) наряду с указанными методами и способами должны применяться следующие дополнительные методы и способы защиты ПД от несанкционированного доступа:

– межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры информационной системы ПД;

– защита ПД при их передаче по каналам связи;

– использование смарт-карт, электронных замков и других носителей информации для надежной идентификации и аутентификации пользователей;

– использование средств антивирусной защиты.

4.1.6. Должна производиться периодическая проверка электронных журналов безопасности, в которых регистрируются события безопасности. К электронным журналам безопасности относятся:

– журналы безопасности операционных систем;

– журналы событий системы управления базами данных;

– журналы событий средств защиты информации;

– журналы событий системы контроля и управления физическим доступом;

– журналы событий прикладного программного обеспечения;

– журналы активных сетевых устройств.

4.1.7. К событиям безопасности в информационной системе ПД относятся следующие события:

– доступ (входа и выхода в систему и доступа к объектам, в том числе неудачные попытки доступа);

– создание и удаление пользователей;

– изменение прав доступа и привилегий;

– подключение и отключение внешних устройств;

– изменение настроек средств защиты;

– события, генерируемые средствами защиты.

4.1.8. В колледже также могут разрабатываться и применяться другие методы защиты информации от несанкционированного доступа, обеспечивающие нейтрализацию угроз безопасности ПД.

4.1.9. Конкретные методы и средства защиты ПД в информационной системе ПД должны определяться на основании нормативно-методических документов ФСТЭК России и ФСБ России, исходя из уровней защищенности ПД в информационной системе ПД и актуальных угроз безопасности ПД.

4.1.10. Все технические средства защиты информации должны быть снабжены инструкциями по эксплуатации.

4.1.11. Должен вестись учет технических средств защиты информации, эксплуатационной и технической документации к ним.

4.1.12. Ответственность за ведение и поддержание в актуальном состоянии журнала учета технических средств защиты информации возлагается на Ответственного за ОБПД.

4.2. Контроль выполнения требований по защите ПД

4.2.1. В соответствии с Требованиями к защите ПД при их обработке в информационных системах ПД, утвержденными постановлением Правительства Российской Федерации от 01.11.2012 № 1119, должен проводиться периодический контроль выполнения требований по обеспечению безопасности ПД (не реже одного раза в три года).

4.2.2. Контроль функций системы защиты производится в рамках мероприятий, описанных в подразделе 7.2 настоящего Положения.

4.2.3. Ответственность контроля функций системы защиты ПД возлагается на Ответственного за ОБПД.

5. Учет съемных электронных носителей персональных данных

5.1. В колледже должен вестись учет защищаемых съемных носителей ПД. К защищаемым носителям ПД относятся следующие:

– носители информации серверов;
– носители информации автоматизированного рабочего места;
– внешние запоминающие устройства (флеш-накопители, карты памяти и т. п.), содержащие ПД.

5.2. Журнал учета защищаемых съемных электронных носителей установленной формы.

5.3. Ответственность за учет защищаемых электронных носителей ПД возлагается на Ответственного за ОБПД.

6. Обязанности персонала

6.1. Функциональные инструкции Ответственного за ООПД и Ответственного за ОБПД расширены с учетом специфики обработки и защиты ПД (Приложение А). Работники, назначаемые на данные роли, ознакомляются под подпись со своими функциональными инструкциями.

6.2. Обязанности Ответственного за ООПД.

6.2.1. В обязанности Ответственного за ООПД входит:

– осуществление внутреннего контроля за соблюдением работниками колледжа законодательства Российской Федерации о ПД, в том числе требований к защите ПД;

– доведение до сведения работников колледже положений законодательства Российской Федерации о ПД, локальных актов по вопросам обработки ПД, требований к защите ПД;

– прием и обработка обращений субъектов ПД и их законных представителей (ведение журнала учета обращений субъектов ПД, анализ правомерности запросов, составление и отправка ответов);

– прием и обработка запросов уполномоченного органа по защите прав субъектов ПД (ведение журнала учета запросов уполномоченного органа по защите прав субъектов ПД, анализ правомерности запросов, составление и отправка ответов);

– ведение и хранение журнала учета проверок уполномоченным органом по защите прав субъектов ПД;

– уведомление уполномоченного органа по защите прав субъектов ПД об обработке ПД, об изменениях в реквизитах оператора ПД;

– уведомление уполномоченного органа по защите прав субъектов ПД по запросу этого органа с предоставлением необходимой информации в течение тридцати дней с даты получения такого запроса.

6.2.2. Ответственный за ООПД обладает следующими полномочиями:

– запрашивать необходимую информацию у руководства и работников колледже, относящуюся к обработке ПД и необходимую для выполнения его обязанностей;

– контролировать выполнение обязанностей Ответственным за ООПД, инженерами по телекоммуникации (техниками), а также выполнение требований законодательства и внутренних нормативных документов колледже, регламентирующих обработку и ОБПД;

– назначать ответственного за уничтожение ПД и контролировать выполнение процедуры уничтожения ПД. Для выполнения уничтожения ПД на бумажном носителе в качестве лица, ответственного за уничтожение ПД, назначается владелец бизнес-процесса, в случае с другими носителями ПД или если обработка ПД осуществляется в информационной системе ПД, в качестве лица, ответственного за уничтожение ПД, назначается владелец информационной системы ПД;

– согласовывать заявки временного или разового допуска работника к работе с ПД в связи со служебной необходимостью.

6.3. Обязанности Ответственного за ООПД

6.3.1. В обязанности Ответственного за ООПД входит:

– предоставление и прекращение доступа пользователей к ПД в информационных системах ПД в соответствии с утвержденным Перечнем должностей работников, допущенных к работе с ПД, или с утвержденными заявками на доступ к ПД;
– управление учетными записями пользователей комплекса информационных систем ПД совместно с инженерами по телекоммуникации (техниками);
– проведение контрольных мероприятий;
– предоставление сведений о ПД Ответственному за ООПД в рамках проведения учета защищаемых носителей и проведения инвентаризации;
– установка, конфигурирование и администрирование аппаратных и программных средств защиты информации комплекса информационных систем ПД;
– поддержание штатной работы комплекса информационных систем ПД совместно с инженерами по телекоммуникации (техниками);
– учет защищаемых носителей ПД;
– учет технических средств защиты информации;
– - периодические ежемесячные проверки журналов безопасности;
– анализ защищенности информационных систем ПД;
– организация процесса обучения работников по направлению обеспечения безопасности ПД;
– участие в проведении внутреннего контроля и служебных расследований фактов нарушения установленного порядка обработки и обеспечения безопасности ПД.

6.3.2. Ответственный за ОБПД обладает следующими полномочиями:

– проводит плановые и внеплановые контрольные мероприятия в целях контроля, изучения и оценки фактического состояния защищенности ПД;
– запрашивает необходимую информацию у очевидцев и подозреваемых лиц при проведении разбирательств по фактам нарушения установленного порядка обработки и обеспечения безопасности ПД.

7. Организация внутреннего контроля обработки и обеспечения безопасности персональных данных

7.1. Цели организации внутреннего контроля

7.1.1. Организация внутреннего контроля процесса обработки ПД в колледже осуществляется в целях изучения и оценки фактического состояния защищенности ПД, своевременного реагирования на нарушения установленного порядка их

обработки, а также в целях совершенствования этого порядка и обеспечения его соблюдения.

7.1.2. Мероприятия по осуществлению внутреннего контроля обработки и обеспечения безопасности ПД направлены на решение следующих задач:

– обеспечение соблюдения работниками колледже требований настоящего Положения и нормативных правовых актов, регулирующих защиту ПД;

– оценка компетентности персонала, задействованного в обработке ПД;

– обеспечение работоспособности и эффективности технических средств информационных систем ПД и средств защиты ПД, их соответствия требованиям уполномоченных органов исполнительной власти по вопросам безопасности ПД;

– выявление нарушений установленного порядка обработки ПД и своевременное предотвращение негативных последствий таких нарушений;

– принятие корректирующих мер, направленных на устранение выявленных нарушений, как в порядке обработки ПД, так и в работе технических средств информационных систем ПД;

– разработка рекомендаций по совершенствованию порядка обработки и обеспечения безопасности ПД по результатам контрольных мероприятий;

– осуществление контроля исполнения рекомендаций и указаний по устранению нарушений.

7.2. Проведение контрольных мероприятий

7.2.1. Контрольные мероприятия (проверки) проводятся на плановой основе, а также при необходимости внепланово.

7.2.2. Решение о необходимости проведения внеплановых контрольных мероприятий принимает Ответственный за ОБПД. Данное решение должно быть обосновано возросшими рисками информационной безопасности для обрабатываемых ПД и при существенных изменениях в среде обработки ПД.

7.2.3. Контрольные мероприятия (проверки) организуются Ответственным за ОБПД.

7.2.4. Плановые проверки проводятся не реже одного раза в полугодие и включают в себя:

– проверку деятельности работников колледже, допущенных к работе с ПД в информационных системах ПД, на соответствие порядку обработки и обеспечения безопасности ПД, установленному Положением по работе с персональными данными и другими нормативными правовыми актами, принятыми в колледже и обязательными для ознакомления и исполнения соответствующими категориями работников;

– проверку работоспособности и эффективности технических средств информационных систем ПД и средств защиты ПД;

– проверку ведения эталонных копий средств защиты;

– проверку соответствия предоставленных прав доступа пользователей к ПД утвержденной матрице доступа;

– проверку минимальной длины и сложности паролей;

– проверку периодичности смены паролей;

– проверку отсутствия на автоматизированных рабочих местах пользователей средств разработки;

– проверку отсутствия на автоматизированных рабочих местах пользователей нештатного программного обеспечения;

– мониторинг журналов протоколирования событий аутентификации.

7.2.5. Ответственный за ОБПД составляет план контрольных мероприятий на полугодие, в котором определяет состав и периодичность проведения проверок на данный период времени.

7.2.6. Результаты проверок оформляются актами. Выявленные в ходе проверок нарушения, а также отметки об их устранении фиксируются в журнале учета выявленных нарушений в порядке обработки и обеспечения безопасности ПД.

7.2.7. Выявленные нарушения расследуются в соответствии с подразделом 7.3.

7.2.8. При необходимости должны быть предложены меры по минимизации последствий выявленных угроз информационной безопасности.

7.2.9. В случае передачи части функций в области информационных технологий сторонним организациям указанные контрольные мероприятия осуществляют эти сторонние организации. Требования по осуществлению контрольных мероприятий указываются в договорах с этими сторонними компаниями.

7.3. Порядок проведения разбирательств

7.3.1. Проведение разбирательств может быть инициировано в одном из следующих случаев:

– обращение субъекта ПД по поводу неправомерных действий с его ПД;

– выявление нарушений работниками колледже в рамках выполнения своих функциональных обязанностей, связанных с обработкой или защитой ПД;

– выявление нарушений, приводящих к снижению уровня защищенности ПД, в ходе проведения проверок состояния защищенности ПД.

7.3.2. В ходе проведения расследования Ответственным за ОБПД проводится опрос очевидцев и подозреваемых лиц, предположительно допустивших нарушение.

7.3.3. В ходе проведения опроса выясняется:

– дата и время совершения нарушения;

– обстоятельства, при которых были совершены действия, приведшие к возникновению нарушения;

– последствия, возникшие вследствие совершения нарушения.

7.3.4. Все опрашиваемые лица должны предоставить объяснительные записки (показания, изложенные на бумажном носителе с подписью опрашиваемого).

7.3.5. Ответственный за ОБПД оценивает последствия, возникшие вследствие совершения нарушения.

7.3.6. По результатам разбирательства Ответственный за ОБПД в течение трех рабочих дней составляет заключение по результатам разбирательств.

7.3.7. В заключении должны быть приведены:

– краткая справка по нарушению, в отношении которого проводилось разбирательство;

– лицо(а), которое совершило(и) нарушение;

– предложения по привлечению виновника к юридической ответственности (дисциплинарной ответственности: замечание, выговор, увольнение; или к гражданско правовой ответственности (взыскание причиненного ущерба) и/или применении к нему мер дисциплинарного воздействия (депремирование, указание на недостатки и т. п.);

– план мероприятий по предотвращению подобных нарушений в будущем (если уместно).

7.3.8. Заключение предоставляется Ответственному за ООПД и согласовывается с директором колледже.

7.3.9. Срок проведения расследования не должен превышать семи рабочих дней.

8. Заключительные положения

8.1. Срок действия Положения не ограничен.

8.2. При изменении законодательства Российской Федерации о персональных данных в Политику вносятся изменения в установленном законом порядке.

Приложение: А. Функциональные инструкции и дополнения в договоры.
Б. Формы согласия субъекта на обработку персональных данных.

Приложение А

ФУНКЦИОНАЛЬНЫЕ ИНСТРУКЦИИ И ДОПОЛНЕНИЯ В ДОГОВОРЫ

А.1. Функциональная инструкция ответственного за обеспечение персональных данных

Назначение работника ответственным за обеспечение персональных данных (далее по тексту – ОПД) осуществляется приказом директора колледже.

Ответственный за ОПД подчиняется непосредственно директору колледже.

В своей деятельности ответственный за ОПД руководствуется:

– действующими нормами международного права и законодательством Российской Федерации;
– уставом колледже;
– организационно-распорядительными документами колледже по вопросам организации обработки и обеспечения безопасности персональных данных (далее по тексту – ПД);
– приказами, распоряжениями директора колледже;
– настоящей должностной инструкцией.

На время отсутствия ответственного за ОПД его обязанности исполняет директор колледже.

Основными задачами ответственного за ОПД являются:

–осуществление внутреннего контроля соблюдения образовательной организацией и ее работниками законодательства Российской Федерации о ПД, в том числе требований к защите ПД;
–доведение до сведения работников колледже положений законодательства Российской Федерации о ПД, локальных актов по вопросам обработки ПД, требований к защите ПД;
–прием и обработка обращений субъектов ПД и их законных представителей (ведение журнала учета обращений субъектов ПД, анализ правомерности запросов, составление и отправка ответов);
–прием и обработка запросов уполномоченного органа по защите прав субъектов ПД (ведение журнала учета запросов уполномоченного органа по защите прав субъектов ПД, анализ правомерности запросов, составление и отправка ответов);
–ведение и хранение журнала учета проверок уполномоченным органом по защите прав субъектов ПД;
–уведомление уполномоченного органа по защите прав субъектов ПД об обработке ПД, об изменениях в реквизитах оператора персональных ПД;

–уведомление уполномоченного органа по защите прав субъектов ПД по запросу этого органа с предоставлением необходимой информации.

Ответственный за ОПД вправе:

–запрашивать необходимую информацию у руководства и работников колледже, относящуюся к обработке ПД и необходимую для выполнения его обязанностей;

–контролировать выполнение обязанностей Ответственным за ОБПД, а также выполнение требований законодательства и внутренних нормативных документов колледже, регламентирующих обработку и ОБПД;

–назначать ответственного за уничтожение ПД и контролировать выполнение процедуры уничтожения ПД;

–согласовывать заявки временного или разового допуска работника к работе с ПД в связи со служебной необходимостью.

А.2. Дополнения в разделы договоров, в соответствии с которыми образовательная организация поручает обработку персональных данных третьим лицам

ТЕРМИНЫ

В настоящем Договоре используются следующие термины, если иное не следует из контекста:

персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

обработка персональных данных («обработка») – любое действие (операцию) 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;

субдоговор и **заключение субдоговора** – процесс, когда Стороны договариваются с третьей стороной о выполнении обязательств в соответствии с настоящим Договором, а «субконтрактор» означает сторону, с которой заключен «субдоговор»;

технические и **организационные меры обеспечения безопасности** – меры, предпринимаемые для обеспечения безопасности персональных данных от случайного или незаконного уничтожения или случайной утраты, неавторизованной модификации, неправомерного раскрытия или доступа, а также от всех иных незаконных форм обработки.

РАЗДЕЛ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Обязанности, связанные с безопасностью:

1) Обработчик обязан совершать какие-либо свои действия в отношении персональных данных, которые он обрабатывает от имени Оператора, исключительно в соответствии с указаниями Оператора.

2) Обработчик обязан принимать надлежащие технические и организационные меры по обеспечению безопасности персональных данных в соответствии с требованиями законодательства Российской Федерации в области персональных данных.

Конфиденциальность:

1) Обработчик соглашается с тем, что он обязан обрабатывать персональные данные от имени Оператора, соблюдая конфиденциальность обработки. В частности, Обработчик соглашается с тем, что, если он не получил письменного согласия от Оператора, он не будет раскрывать персональные данные, переданные Обработчику Оператором/для Оператора/от имени Оператора третьим лицам.
2) Обработчик не должен использовать персональные данные, переданные ему Оператором, кроме как в соответствии с существом услуг, оказываемых им Оператору.

Заключение «субдоговора»:

1) Обработчик не должен заключать «субдоговор» по исполнению своих обязательств, налагаемых настоящим Договором, без предварительного письменного согласия Оператора.
2) В том случае если Обработчик с согласия Оператора заключает «субдоговор», он обязан заключать этот договор в письменной форме, а сам договор должен содержать все те обязательства в отношении безопасности обработки, которые накладываются на Обработчика в соответствии с настоящим Договором.
3) Если «субконтрактор» не в состоянии выполнять свои обязательства, вытекающие из «субдоговора», Обработчик несет полную ответственность перед Оператором за выполнение обязательств, накладываемых на него настоящим Договором.

Порядок действий с персональными данными после прекращения действия Договора.

В течение 5 дней со дня окончания действия настоящего Договора Обработчик обязан по указанию Оператора:

– вернуть все персональные данные, переданные для обработки Обработчику Оператором, или
– по указанию Оператора уничтожить все персональные данные, если это не запрещено законодательством, или
– выполнить все дополнительные соглашения между Сторонами в части возвращения или уничтожения данных.

А.3. Дополнения в разделы трудовых договоров об обеспечении безопасности персональных данных

В раздел трудовых договоров (функциональных инструкций) персонала информационных, закрепляющий должностные обязанности, необходимо включить следующий пункт:

1) При работе с информационными системами ПД следует руководствоваться требованиями к порядку обработки и обеспечения безопасности ПД, закрепленными в настоящем Положении.

В раздел «Ответственность» трудовых договоров (функциональных инструкций) работников колледже, допущенных к обработке ПД для выполнения своих функциональных обязанностей, необходимо включить следующие пункты:

1) Работник колледже несет ответственность за обеспечение конфиденциальности ПД, ставших ему известными в связи с выполнением функциональных обязанностей.

2) Работник колледже несет персональную ответственность за соблюдение требований по обработке и обеспечению безопасности ПД, установленных в Положении по организации и проведению работ по обеспечению безопасности ПД при их обработке в информационных системах ПД колледже.

3) В случае нарушения установленного порядка обработки и обеспечения безопасности ПД, несанкционированного доступа к персональным данным, раскрытия ПД и нанесения колледже, его работникам или клиентам материального или иного ущерба виновные лица несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Приложение Б

Формы согласия субъекта на обработку его персональных данных

Б.1. Типовая форма согласия родителей (законных представителей) обучающихся на обработку персональных данных

СОГЛАСИЕ РОДИТЕЛЯ (ЗАКОННОГО ПРЕДСТАВИТЕЛЯ) НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ НЕСОВЕРШЕННОЛЕТНЕГО

Я, _____(ФИО), проживающий по адресу _____, паспорт серия_____ № _____ выдан (кем и когда) _____ __, тел.:_____, адрес электронной почты:_____ являюсь законным представителем несовершеннолетнего _____ (ФИО) на основании ст. 64 п. 1 Семейного кодекса РФ .

Настоящим даю свое согласие на обработку в ПОЧУ «КИД» персональных данных моего несовершеннолетнего ребенка (подопечного) _____, относящихся исключительно к перечисленным ниже категориям персональных данных:

- данные свидетельства о рождении/данные документа, удостоверяющего личность: ФИО; пол; дата рождения; тип, серия, номер документа, удостоверяющего личность; гражданство.
- медицинские сведения: данные медицинской карты; сведения о состоянии здоровья; отнесение к категории лиц с ОВЗ, детей-инвалидов; сведения о прохождении медосмотров; сведения об освоении адаптированной образовательной программы; сведения о наличии заключения ЦПМПК;
- СНИЛС;
- адрес проживания/пребывания ребенка;
- номер телефона и адрес электронной почты;
- учебные достижения ребенка: сведения об успеваемости; учебные работы ребенка; форма обучения, номер класса (группы), наличие/отсутствие льгот, данные о получаемом дополнительном образовании, форма ГИА, наличие допуска и перечень предметов, выбранных для сдачи ГИА, место сдачи ГИА, результаты ГИА (в том числе итогового сочинения, изложения), содержание поданной апелляции и результаты ее рассмотрения;
- фото- и видео- изображение;

а также моих персональных данных, а именно:

- ФИО, фотоизображения (при использования информационной системы проход и питание (ИСПП).

Я даю согласие на использование персональных данных моего ребенка (подопечного) исключительно в следующих целях:

- обеспечения защиты конституционных прав и свобод моего ребенка (подопечного);

- обеспечения соблюдения нормативных правовых актов Российской Федерации и города Москвы;

- обеспечения безопасности обучающихся в период нахождения на территории колледже;

- обеспечения организации учебного процесса для ребенка, в том числе актуализация оценок успеваемости в электронном дневнике;

- обеспечения организации внеурочной деятельности, экскурсий, олимпиад и спортивных соревнований, и иных знаковых мероприятий;

- ведения статистики;

- размещения фотоизображения на официальном сайте ПОЧУ «КИД» и социальных сетях в рамках образовательного процесса, внеурочной деятельности, экскурсий, олимпиад и спортивных соревнований, и иных знаковых мероприятий на территории колледже;

- видеосъемки и размещения видеоматериалов на официальном сайте ПОЧУ «КИД» и социальных сетях в рамках внеурочной деятельности, экскурсий, олимпиад, спортивных соревнований, и иных знаковых мероприятий на территории колледже;

- видеосъемки и размещения видеоматериалов на официальном сайте ПОЧУ «КИД» и социальных сетях в рамках образовательного процесса (в случае размещения видеонаблюдения в группах – в целях предоставления услуг видеонаблюдения родителям (законным представителям) обучающихся);

- размещения на официальном сайте информации об успехах и достижениях обучающихся;

- размещения приказа о зачислении обучающихся (во исполнение требований Приказа Министерства образования № 36 от 6 марта 2014 года «Об утверждении Порядка приема на обучение по образовательным программам среднего профессионального образования» - для ГБОУ СПО);

- передачи сведений в федеральные и региональные информационные системы в целях обеспечения проведения процедур оценки качества образования – независимых диагностик, мониторинговых исследований, государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования (в соответствии с правилами, утвержденными постановлением Правительства Российской Федерации от 31 августа 2013 г. № 755), ведения федерального реестра сведений документов об образовании и(или) квалификации, документов об обучении (в соответствии с Постановление Правительства Российской Федерации от 26 августа 2013 года № 729);

- работы с подсистемами КИС ГУСОЭВ;

- начисления стипендии (для обучающихся по программам среднего профессионального и высшего образования) и иных выплат, в том числе социальных;

- контроля посещения занятий;

- предоставления информации для оформления проездных документов.

Настоящее согласие предоставляется на осуществление ПОЧУ «КИД» следующих действий в отношении персональных данных ребенка: сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование (только в указанных выше целях), обезличивание, блокирование (не включает возможность ограничения моего доступа к персональным данным ребенка), а также осуществление любых иных действий, предусмотренных действующим законодательством Российской Федерации.

Я не даю согласия на какое-либо распространение персональных данных ребенка (подопечного), в том числе на передачу персональных данных ребенка каким-либо третьим лицам, включая физических и юридических лиц, государственных органов и органов местного самоуправления, за исключением передачи персональных данных следующим организациям:

- Департаменту образования и науки города Москвы, в том числе подведомственным ему организациям;

- Департаменту информационных технологий города Москвы, в том числе подведомственным ему организациям;

- Федеральной службе по надзору в сфере образования и науки, в том числе подведомственным ему организациям;

Обработка персональных данных должна осуществляться с соблюдением требований, установленных законодательством Российской Федерации и только для целей, указанных выше. ПОЧУ «КИД» обязан осуществлять защиту персональных данных ребенка, принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, модифицирования, блокирования, копирования, распространения, а также от иных неправомерных действий в отношении данной информации.

Обработка персональных данных моего ребенка для любых иных целей и любым иным способом, включая распространение и передачу их иным лицам или иное их разглашение может осуществляться только с моего особого письменного согласия в каждом отдельном случае.

Защита внесенной информации осуществляется с соблюдением требований, установленных законодательством Российской Федерации. Хранение, обработка, а также обмен информацией осуществляются после принятия необходимых мер по защите указанной информации. В случае нарушения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» ПОЧУ «КИД» несет ответственность, предусмотренную законодательством Российской Федерации.

Данное Согласие может быть отозвано в любой момент по моему письменному заявлению.

Мне разъяснено, что отзыв настоящего согласия может затруднить или сделать невозможным возобновление обработки персональных данных и их подтверждение.

Я подтверждаю, что, давая настоящее согласие, я действую по своей воле и в интересах моего ребенка (подопечного), законным представителем которого я являюсь.

_____ _____

подпись *иоф*

_____

дата (день, месяц, год)

Б.2. Форма согласия работника на обработку персональных данных

СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ
РАБОТНИКА ПОЧУ «КИД»

Я,_____,
(*фамилия, имя, отчество полностью*), зарегистрированного по адресу_____, паспорт серия_____№____ выдан (кем) _____(когда) даю свое согласие на обработку своих персональных данных в целях:

- обеспечения защиты моих конституционных прав и свобод;
- обеспечения соблюдения законов и иных нормативных правовых актов;
- заключения и регулирования трудовых отношений и иных непосредственно связанных с ними отношений;
- отражения информации в кадровых документах;
- начисления заработной платы;
- предоставления льгот, предусмотренных трудовым и налоговым законодательством;
- исчисления и уплаты, предусмотренных законодательством РФ налогов, сборов и взносов на обязательное социальное и пенсионное страхование;
- представления работодателем установленной законодательством отчетности в отношении физических лиц, в том числе сведений персонифицированного учета в Пенсионный фонд РФ, сведений подоходного налога в ФНС России, сведений в ФСС РФ;
- перечисления заработной платы;
- оформления полиса ДМС;
- предоставления налоговых вычетов;
- обеспечения моей безопасности;
- оперативного доведения до меня информации со стороны ПОЧУ «КИД»;
- контроля количества и оценки качества выполняемой мной работы;
- размещения фото и видеоизображений на официальном сайте ПОЧУ «КИД» для освещения образовательного процесса, внеурочной деятельности, экскурсий, олимпиад и спортивных соревнований, и иных знаковых мероприятий;
- передачи сведений в федеральные и региональные информационные системы в целях обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования (в соответствии с правилами, утвержденными Постановлением Правительства Российской Федерации от 31 августа 2013 г. № 755).

Перечень моих персональных данных, на обработку которых я даю согласие:

- фамилия, имя, отчество;
- пол, возраст;
- дата и место рождения, гражданство;
- паспортные данные (серия, номер, кем и когда выдан);
- фото-, видео- изображения;
- сведения о социальных льготах, о состоянии здоровья, о результатах медицинских осмотров и о профилактических прививках;

- сведения о временной нетрудоспособности, о характере полученных травм на работе;
- наличие (отсутствие) судимости и (или) факта уголовного преследования;
- сведения об условиях труда на рабочем месте;
- адрес регистрации по месту жительства и адрес фактического проживания;
- номер телефона (домашний, мобильный) и адрес электронной почты;
- сведения об образовании (квалификация, профессиональная подготовка, повышение квалификации);
- результаты прохождения аттестации;
- семейное положение, состав семьи;
- отношение к воинской обязанности;
- сведения о трудовом стаже, наличие наград, поощрений и почетных званий, предыдущих местах работы, доходах с предыдущих мест работы;
- должность;
- размер заработной платы;
- сведения об открытых банковских счетах, на которые перечисляется заработная плата в ПОЧУ «КИД»;
- сведения о налоговых отчислениях и сборах;
- номер СНИЛС;
- ИНН;
- информация о приеме, переводе, увольнении и иных событиях, относящихся к моей трудовой деятельности в ПОЧУ «КИД»;
- сведения о доходах в ПОЧУ «КИД»;
- опыт в проведении ГИА в предыдущие годы
- сведения о деловых и иных личных качествах, носящих оценочный характер.

Я не даю согласия на какое-либо распространение моих персональных данных и их передачу третьим лицам, включая физических и юридических лиц государственных органов и органов местного самоуправления, за исключением передачи персональных данных следующим организациям:

- Департамент образования и науки города Москвы, в том числе подведомственные ему организации;
- Департамент информационных технологий города Москвы, в том числе подведомственные ему организации;
- Федеральная служба по надзору в сфере образования и науки, в том числе в том числе подведомственные ему организации;
- Федеральная служба по труду и занятости;
- Пенсионный фонд России;
- Федеральная налоговая служба России;
- Фонд социального страхования России;
- Московская городская организация Профсоюза работников народного образования и науки РФ.

Обработка персональных данных должна осуществляться с соблюдением требований, установленных законодательством Российской Федерации и только для целей, указанных выше. ПОЧУ «КИД» обязано осуществлять защиту моих персональных данных, принимать необходимые организационные и технические меры для защиты моих персональных данных от неправомерного или случайного доступа к ним, уничтожения, модифицирования, блокирования, копирования, распространения, обезличивание, а также от иных неправомерных действий в отношении данной информации.

Обработка моих персональных данных для любых иных целей и любым иным способом, включая распространение и передачу их иным лицам, или иное их разглашение может осуществляться только с моего письменного согласия в каждом отдельном случае.

Защита внесенной информации должна осуществляться с соблюдением требований, установленных законодательством Российской Федерации. Хранение и обработка информации, а также обмен информацией должны осуществляться после принятия необходимых мер по защите указанной информации. В случае нарушения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» ПОЧУ «КИД» должна нести ответственность, предусмотренную Кодексом об административных правонарушениях РФ, Трудовым кодексом РФ, Уголовным кодексом РФ.

Данное Согласие действует до достижения целей обработки персональных данных в ПОЧУ «КИД» или в течение срока хранения информации. Данное Согласие может быть отозвано в любой момент по моему письменному заявлению в его части или полном объеме.

Я подтверждаю, что, давая настоящее согласие, я действую по своей воле и в своих интересах.

_____ _____

подпись *иоф*

_____

дата (день, месяц, год)

Приложение В

Форма акта об уничтожении персональных данных

УТВЕРЖДАЮ
Директор
ПОЧУ «КИД»
_____ _____
подпись *иоф*
_____ _____20_ г.

А К Т

_____№ _____

Об уничтожении персональных данных

№ п/п	Дата	Место и форма хранения персональных данных	Тип носителя персональных данных и его регистрационный номер / уничтожаемые персональные данные

Всего уничтожено носителей (прописью): _____.

Уничтожение произведено путем _____

_____.

Ответственный за уничтожение

_____
фамилия имя отчество, должность

_____ _____
подпись *иоф*

_____
дата (день, месяц, год)