УТВЕРЖДАЮ

Директор МБУ ЦППМИСП

Миллеровского района

_____КовалеваА.Н.

«29» 09 2023г

ПОЛОЖЕНИЕ
Об обработке персональных данных с использованием средств автоматизации в МБУ ЦППМиСП

I. Общие положения

1.1.Положение об особенностях обработки персональных данных с использованием средств автоматизации (далее-Положение) определяет особенности и их порядок обработки персональных данных при их обработке с использованием средств автоматизации в МБУ ЦППМиСП.

1.2.Положение разработано во исполнение Политики в отношении обработки персональных данных и в соответствии ст. 16 Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» ст.18.1 п.2, ст. 19 п. 1,2 Федеральный закон «О персональных данных» от 27.07.2006 г. № 152-ФЗ п. 1б, в, е. Постановление Правительства РФ «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» от 20.03.2012 г. № 211.

1.3.Цели разработки Положения:

1.3.1.Определение порядка обработки персональных данных участников образовательного процесса, а также иных субъектов персональных данных, персональные данные которых подлежат обработке на основании полномочий МБУ ЦППМиСП.

1.3.2. Обеспечение защиты прав и свобод человека и гражданина, в т.ч. сотрудников, учащихся и их родителей (законных представителей) МБУ ЦППМиСП, при обработке их персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.3.3.Установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.4.К любой информации, содержащей персональные данные субъекта, применяется режим конфиденциальности, за исключением:

-Обезличенных персональных данных;

-Общедоступных персональных данных.

1.5.Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении срока их хранения, если иное не определено законом Российской Федерации.

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1.6.**Блокирование персональных данных-** временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных) (ст. 3 ФЗ РФ от 27.07.2006 г. № 152 –ФЗ «О персональных данных»).

1.7.**Информационная система персональных данных (ИСПДн)** – совокупность содержащихся в базе данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств (ст. 3 ФЗ РФ от 27.07.2006 г. № 152 –ФЗ «О персональных данных»).

1.8.**Документальная информация-** зафиксированная на материальном носителе путем документирования информации с реквизитами, позволяющими определить такую информацию или ее материальный носитель (ст. 2 ФЗ РФ от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»).

1.9.**Информация** – сведения (сообщения, данные) независимо от формы их представления (ст. 2 ФЗ РФ от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»).

1.10.**Обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных (ст. 3 ФЗ РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных»).
1.11.**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 (ст. 3 ФЗ РФ от 27.07.2006 г. № 152 –ФЗ «О персональных данных»).
1.12.**Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных) (ст. 3 ФЗ РФ от 27.07.2006 г. № 152 –ФЗ «О персональных данных»).
1.13.**Распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц (ст. 3 ФЗ РФ от 27.07.2006 г. № 152 – ФЗ «О персональных данных»).
1.14.**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 (ст. 3 ФЗ РФ от 27.07.2006 г. № 152 –ФЗ «О персональных данных»).

2.СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1.Состав персональных данных, обрабатываемых МБУ ЦППМиСП, определяется «Перечнем сведений, содержащих персональные данные» (Приложение 1).

3.ПОРЯДОК ПОЛУЧЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1.Персональные данные следует получать непосредственно у субъекта, либо у законного представителя.
3.2.Перед началом обработки персональных данных необходимо получить у субъекта или его законного представителя согласие на обработку персональных данных в письменной форме, в соответствии с утвержденной МБУ ЦППМиСП формой такого Согласия.
3.3.Комплекс документов, сопровождающий процесс оформления трудовых отношений сотрудника с МБУ ЦППМиСП при его приеме, переводе или увольнении:
3.3.1.Информация, представляемая сотрудником при поступлении на работу в МБУ ЦППМиСП должна иметь документальную форму. При заключении трудового договора в соответствии со статьей 65 Трудового кодекса Российской Федерации лицо, поступающее на работу, представляет работодателю:
3.3.1.1.Паспорт или иной документ, удостоверяющий личность;
3.3.1.2.Трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или сотрудник поступает на работу на условиях совместительства, либо трудовая книжка у сотрудника отсутствует в связи с ее утратой или по другим причинам;
3.3.1.3.Страховое свидетельство государственного пенсионного страхования;
3.3.1.4.Документы воинского учета - для военнообязанных и лиц, подлежащих воинскому учету;
3.3.1.5.Документ об образовании, о квалификации или наличии специальных знаний - при поступлении на работу, требующую специальных знаний или специальной подготовки;
3.3.1.6.Свидетельство о присвоении ИНН (при его наличии у сотрудника).
3.3.2.В МБУ ЦППМиСП создаются и хранятся следующие группы документов, содержащие персональные данные сотрудников в единичном или сводном виде:
3.3.2.1.Документы, содержащие персональные данные сотрудников (комплексы документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении; комплекс материалов по анкетированию, тестированию; проведению собеседований с кандидатом на должность; подлинники и копии приказов по личному составу; личные дела и трудовые книжки сотрудников; дела, содержащие основания к приказу по личному составу; дела, содержащие материалы аттестации сотрудников; служебных расследований; справочно-информационный банк данных по персоналу (картотеки, журналы); подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству МБУ ЦППМиСП,

руководителям структурных подразделений; копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения);
3.3.2.2.Документация МБУ ЦППМиСП, положения, должностные инструкции сотрудников, приказы директора МБУ ЦППМиСП;
3.3.2.3.Документы по планированию, учету, анализу и отчетности в части работы с персоналом МБУ ЦППМиСП.
3.4.Комплекс документов, сопровождающий процесс оформления отношений с учащимися, их родителями или законными представителями при приеме, переводе и отчислении определяется согласно Положения о порядке приема граждан в МБУ ЦППМиСП, а также Положений о переводе и отчислении учащихся.

4.ПОРЯДОК ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1.Хранение электронных носителей (дискет, дисков и т.п.), содержащих персональные данные, должно осуществляться в МБУ ЦППМиСП в специальных папках, закрытых шкафах или сейфах, в порядке, исключающем доступ к ним третьих лиц.
4.2.Безопасность персональных данных при их обработке с использованием технических и программных средств обеспечивается с помощью системы защиты персональных данных, включающей в себя организационные меры и средства защиты информации, удовлетворяющие устанавливаемым в соответствии с законодательством РФ требованиям, обеспечивающим защиту информации.
4.3.Обработка персональных данных в МБУ ЦППМиСП осуществляется до утраты правовых оснований обработки персональных данных. Перечень нормативно-правовых актов, определяющих основания обработки персональных данных в МБУ ЦППМиСП определяются «Перечнем сведений, содержащих персональные данные» (Приложение 1).

5. ПОРЯДОК ИСПОЛЬЗОВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1.Обработка персональных данных может осуществляться исключительно в целях:
5.1.1.Исполнения положений нормативных актов.
5.1.2.Принятия решения о трудоустройстве кандидата в МБУ ЦППМиСП.
5.1.3.Заключения и выполнения обязательств по трудовым договорам, договорам гражданско-правового характера и договорам с контрагентами.
5.1.4.Приема родителей (законных представителей), рассмотрения жалоб, обращений, заявлений и предложений всех участников образовательного процесса.
5.1.5.Рассмотрения Представлений к награждению сотрудников МБУ ЦППМиСП.
5.1.6.Трудовых (договорных) отношений; приема граждан, рассмотрения жалоб, обращений и предложений граждан и в случаях, установленных законодательством Российской Федерации.
5.2.При определении объема и содержания, обрабатываемых персональных данных, МБУ ЦППМиСП должно руководствоваться Конституцией Российской Федерацией, Трудовым кодексом Российской Федерации, Федеральным законом «О персональных данных» от 27.07.2006 года № 152-ФЗ, Гражданским кодексом Российской Федерации и иными нормативно-правовыми актами Российской Федерации, а также настоящим Положением.

6.ПОРЯДОК ПЕРЕДАЧИ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1.Передавать персональные данные субъектов допускается только тем сотрудникам, которые имеют допуск к обработке персональных данных.
6.2.Предоставление персональных данных допускается в случаях передачи Федеральной налоговой службе, Пенсионному фонду России, Негосударственным пенсионным фондам, Страховым компаниям, Страховым медицинским компаниям, Фонду социального страхования, Отделу военного комиссариата Ростовской области, ГУ МВД России по Ростовской области, Федеральной службе Государственной регистрации, кадастра и картографии (Росреестр), Управлению образования Миллеровского района, МОиН Ростовской области. Прокуратуре при официальном запросе, раскрытии данных правоохранительным органам при наличии законных оснований.
6.3.Не допускается распространение персональных данных субъекта.

7.ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1.Защита персональных данных субъекта от неправомерного их использования или утраты обеспечивается МБУ ЦППМиСП за счет своих средств.

7.2.Защита персональных данных должна вестись по трем взаимодополняющим направлениям:
7.2.1.Проведение организационных мероприятий:
7.2.1.1.Разработка и внедрение внутренних организационно-распорядительных документов, регламентирующих обработку и защиту персональных данных субъектов;
7.2.1.2.Ознакомление сотрудников с законодательством Российской Федерации и внутренними нормативными документами, получение обязательств, касающихся обработки персональных данных;
7.2.1.3.Организация учета носителей персональных данных;
7.2.1.4.Разработка модели угроз безопасности персональным данным;
7.2.1.5.Проведение обучения сотрудников вопросам защиты персональных данных.
7.2.2.Программно-аппаратная защита:
7.2.2.1.Внедрение программно-аппаратных средств защиты информации, прошедших в соответствии с Федеральным законом № 184 от 27.12.2002 г. «О техническом регулировании» оценку соответствия;
7.2.3.Инженерно-техническая защита:
7.2.3.1.Установка сейфов или запирающихся шкафов для хранения носителей персональных данных;
7.2.3.2.Установка усиленных дверей, сигнализации, режима охраны здания и помещений, в которых обрабатываются персональные данные.
7.3. Определение конкретных мер, планирование и контроль выполнения мероприятий по защите персональных данных осуществляет ответственный за организацию обработки персональных данных в соответствии с законодательством в области защиты персональных данных и локальными нормативно-правовыми актами МБУ ЦППМиСП.
7.4.Организацию и контроль защиты персональных данных в структурном подразделении ПМПК осуществляет заместитель директора.

8.ПОРЯДОК ПРЕДОСТАВЛЕНИЯ ДОСТУПА К ПЕРСОНАЛЬНЫМ ДАННЫМ

8.1.Доступ к персональным данным субъекта могут иметь только те сотрудники, которым персональные данные необходимы в связи с исполнением ими трудовых обязанностей. Перечень таких сотрудников отражен в «Приказе об утверждении списка должностных лиц, которым необходим доступ к персональным данным, обрабатываемым в информационных системах».
8.2.Процедура оформления допуска к персональным данным представляет собой следующую строгую последовательность действий:
8.2.1.Ознакомление сотрудника с настоящим Положением, «Инструкцией о порядке работы с персональными данными» и другими локальными нормативно-правовыми актами, касающимися обработки персональных данных;
8.3.Каждый сотрудник должен иметь доступ к минимально необходимому набору персональных данных субъектов, необходимых ему для выполнения служебных (трудовых) обязанностей.
8.4.Сотрудникам, не имеющим надлежащим образом оформленного допуска, доступ к персональным данным субъектов запрещается.
8.5.Сотрудники, которым доступ к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных обязанностей (далее-пользователи), для получения доступа к информационной системе направляют письменный запрос на имя ответственного за организацию обработки персональных данных.

9.ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ

9.1.При обработке персональных данных в информационной системе должно быть обеспечено:
9.1.1.Проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
9.1.2.Своевременное обнаружение фактов несанкционированного доступа к персональным данным;
9.1.3.Недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
9.1.4.Возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
9.1.5.Постоянный контроль над обеспечением уровня защищенности персональных данных.
9.2.Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включает в себя:
9.2.1.Определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

9.2.2.Разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;
9.2.3.Проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;
9.2.4.Установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;
9.2.5.Обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
9.2.6.Учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
9.2.7.Учет лиц, допущенных к работе с персональными данными в информационной системе;
9.2.8.Контроль по соблюдению условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
9.2.9.Разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.
9.2.10.Описание системы защиты персональных данных.
9.3.Осуществление мероприятий по обеспечению безопасности персональных данных при их обработке в информационной системе уполномоченным лицом возлагается на администратора безопасности ИСПДн МБУ ЦППМиСП.
9.4.При обнаружении нарушений порядка предоставления персональных данных уполномоченное лицо незамедлительно приостанавливает предоставление персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин.
9.5.Иные требования по обеспечению безопасности информации и средств защиты информации в МБУ ЦППМиСП выполняются в соответствии с требованиями федеральных органов исполнительной власти и органов исполнительной власти Ростовской области.

10.ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

10.1.Под техническими средствами, позволяющими осуществлять обработку персональных данных понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных, программные средства, средства защиты информации, применяемые в информационных системах.
10.2.Безопасность персональных данных достигается путем исключения 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.
10.3.Средства защиты информации, применяемые в информационных системах, в обязательном порядке проходят процедуру оценки соответствия в установленном законодательством РФ порядке.
10.4.Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер, а также применения технических и (или) программных средств.
10.5.Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.
10.6.Безопасность персональных данных при их обработке в информационной системе персональных данных обеспечивает специалист, ответственный за организацию обработки персональных данных в ИСПДн (администратор безопасности ИСПДн).
10.7.При обработке персональных данных в информационной системе должно быть обеспечено:
10.7.1.Проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
10.7.2.Своевременное обнаружение фактов несанкционированного доступа к персональным данным;

10.7.3.Недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
10.7.4.Возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
10.7.5.Постоянный контроль над обеспечением уровня защищенности персональных данных.
10.8.Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают:
10.8.1.Определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;
10.8.2.Разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;
10.8.3.Проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;
10.8.4.Установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;
10.8.5.Обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
10.8.6.Учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
10.8.7.Учет лиц, допущенных к работе с персональными данными в информационной системе;
10.8.8.Контроль по соблюдению условий использования средств защиты информации, предусмотренных эксплуатационной и технической документации;
10.8.9.Разбирательство и составление заключений по факту несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

11.ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ОБРАБОТКУ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ

11.1.Ответственность за соблюдение требований по защите информации ограниченного доступа и надлежащего порядка проводимых работ возлагается на пользователей ИСПДн, администратора безопасности ИСПДн и ответственного за организацию обработки персональных данных МБУ ЦППМиСП.
11.2.Сотрудники МБУ ЦППМиСП, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.
11.2.1.Разглашение персональных данных субъекта (передача их посторонним лица, в том числе другим сотрудникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных настоящим Положением, локальными нормативно-правовыми актами (приказами, распоряжениями) МБУ ЦППМиСП, влечет наложение на сотрудника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Сотрудник МБУ ЦППМиСП, имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность (в соответствии с п.7 ст. 243 Трудового кодекса РФ).
11.2.2.В отдельных случаях, при разглашении персональных данных, сотрудник, совершивший указанный проступок, несет ответственность в соответствии со статьей 13.14 Кодекса об административных правонарушениях РФ.
11.2.3.В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии со ст. 137 Уголовного кодекса РФ.