

**Муниципальное бюджетное общеобразовательное учреждение
«Центр образования № 44 имени Маршала Советского Союза Г.К.Жукова»**

ПРИНЯТО

Управляющим советом МБОУ ЦО № 44

Протокол № 1 от 15.01.2025

УТВЕРЖДЕНО

приказом МБОУ ЦО № 44

от 15.01.2025 № 41-о

**ПОЛОЖЕНИЕ
О ХРАНЕНИИ И ИСПОЛЬЗОВАНИИ
ПЕРСОНАЛЬНЫХ ДАННЫХ
РАБОТНИКОВ И ОБУЧАЮЩИХСЯ,
ВОСПИТАННИКОВ**

СОГЛАСОВАНО

Председатель первичной
профсоюзной организации
МБОУ ЦО № 44

_____ Е.В. Косяченко

г. Тула, 2025 год

1. Общие положения

1.1. Настоящее Положение о хранении и использовании персональных данных работников и обучающихся, воспитанников (далее – Положение) разработано в соответствии с:

- частью 1 статьи 23, статьи 24 Конституции Российской Федерации,
- Гражданским кодексом Российской Федерации,
- главой 14 Трудового кодекса Российской Федерации,
- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информатизации и защите информации»,
- Федеральным законом от 27.07.2006 № 152 – ФЗ «О персональных данных»,
- Указом Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера»,
- постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»,
- постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»,
- приказом Федеральной службы по техническому и экспертному контролю Российской Федерации от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»,
- Уставом муниципального бюджетного общеобразовательного учреждения «Центр образования № 44 имени Маршала Советского Союза Г.К. Жукова» (далее - Центр).

1.2. Целью настоящего Положения является регламентация технологического и организационного процесса защиты персональных данных в Центре.

1.3. Настоящее Положение является обязательными для исполнения всеми работниками, имеющими доступ к персональным данным.

1.4. Термины и определения, используемые в настоящем Положении:

1.4.1. Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.4.2. Использование персональных данных – действия (операции) с персональными данными, совершаемые Оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

1.4.3. Конфиденциальность персональных данных – обязательное для соблюдения Оператором требование не допускать распространения

персональных данных без согласия субъекта персональных данных или наличия иного законного основания.

1.4.4. 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.

1.4.5. Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе.

1.4.6. Оператор персональных данных (далее Оператор) – юридическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

1.4.7. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Персональные данные работника – информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника.

Персональные данные обучающихся, воспитанников – информация, необходимая Центру в связи с отношениями, возникающими между обучающимся, воспитанником и его родителями (законными представителями) и Центром.

1.4.8. Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

1.4.9. Сотрудник (работник) – физическое лицо, состоящее в трудовых отношениях с Оператором.

1.4.10. Субъект – физическое лицо, обладатель собственных персональных данных.

2. Принципы защиты персональных данных субъектов

2.1. В целях защиты персональных данных субъектов создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лиц, пытающихся совершить несанкционированный доступ и овладение персональными данными. Целью и результатом несанкционированного доступа к персональным данным субъектов может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внедрение вредоносных программ, фальсификация содержания реквизитов документа и др.

2.2. Основным источником несанкционированного доступа к персональным данным является персонал, работающий с документами и базами данных.

2.3. Состав обрабатываемых персональных данных приведён в Перечне персональных данных, обрабатываемых в МБОУ ЦО № 44.

2.4. Посторонние лица не должны знать информацию о распределении функций, рабочих процессах, технологии составления, оформления, ведения и хранения документов, дел и рабочих материалов в информационных системах персональных данных. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности Оператора, например посетители, работники других организационных структур.

2.5. Для обеспечения защиты персональных данных сотрудников Центр соблюдает следующие организационно-технические меры:

2.5.1. Регламентирует состав работников, функциональные обязанности которых требуют доступа к персональным данным, и процесс предоставления такого доступа.

2.5.2. Регламентирует порядок приёма, учёта и контроля деятельности посетителей.

2.5.3. Поддерживает порядок охраны зданий и помещений.

2.5.4. Осуществляет периодический контроль обеспечения защищённости персональных данных субъектов.

2.5.5. Соблюдает требования к защите персональных данных субъектов при интервьюировании и беседах.

2.6. В случаях обнаружения несоблюдения условий хранения носителей персональных данных и/или несоблюдения использования средств защиты информации, а также в случае обнаружения нарушения порядка предоставления персональных данных, производится разбирательство и составляется заключение по выявленным фактам.

3. Перечень мер по защите персональных данных при их автоматизированной обработке

3.1. Для обеспечения защиты персональных данных при их обработке в информационных системах принимаются следующие меры:

3.1.1. Определяются угрозы безопасности персональным данным при их обработке, формирование на их основе модели угроз.

3.1.2. Разрабатывается на основе модели угроз система защиты персональных данных, обеспечивающая нейтрализация предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем.

3.1.3. Проверяется готовность средств защиты информации к использованию с составлением заключений о возможности их эксплуатации.

3.1.4. Устанавливаются и вводятся в эксплуатацию средства защиты информации в соответствии с эксплуатационной и технической документацией.

3.1.5. Обучаются лица, использующие средства защиты информации, применяемые в информационных системах, правилам работы с ними.

3.1.6. Осуществляется:

- учёт применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
- учёт лиц, допущенных к работе с персональными данными в информационной системе;
- контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- 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 защищённости персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

3.2. Порядок доступа работников Центра в помещения, в которых ведётся обработка персональных данных, представлен в приложении 1 к настоящему Положению.

4. Перечень мер по защите персональных данных, обрабатываемых без использования средств автоматизации

Для обеспечения защиты материальных носителей, содержащих персональные данные субъектов, Оператор:

4.1. Доводит до сотрудников, осуществляющих обработку персональных данных субъектов на материальных носителях, информацию об особенностях и правилах осуществления такой обработки.

4.2. Запрещает вынос за пределы Центра носителей, содержащих персональные данные субъектов, за исключением случаев, установленных законодательством.

4.3. Хранит носители, содержащие персональные данные, только в сейфах (шкафах), с надёжными средствами защиты, предотвращающими неконтролируемый доступ к ним. Места хранения носителей определяются приказом директора Центра.

4.4. Обеспечивает учёт материальных носителей, содержащих персональные данные. Система учёта должна предоставлять возможность контроля над местонахождением каждого материального носителя.

4.5. Организационно исключает необоснованное ознакомление с персональными данными лиц, не имеющих соответствующих полномочий.

4.6. Обеспечивает защиту от несанкционированного доступа и копирования персональных данных на материальных носителях, согласно организационным и распорядительным документам, принятым в Центре.

5. Контроль защищённости персональных данных субъектов

5.1. Центр осуществляет периодический контроль выполнения организационно-технических мер, а также контроль защищённости информационных ресурсов, содержащих персональные данные.

5.2. Виды контроля состояния защищённости персональных данных субъектов, обрабатываемых в Центре:

5.2.1. Предварительный контроль (оценочная проверка обоснованности мер защиты персональных данных до начала их обработки). Осуществляется с целью своевременного выявления и предотвращения предпосылок возможных нарушений требований или норм защиты персональных данных.

5.2.2. Текущий контроль (проверка в процессе обработки персональных данных). Осуществляется с целью своевременного выявления возникающих трудностей и недостатков реализации, принятых мер защиты персональных данных и выработки мероприятий по их устранению.

5.2.3. Контроль эффективности. Проводится с целью проверки соответствия количественных или качественных показателей эффективности мероприятий по защите персональных данных установленным требованиям или нормам эффективности защиты;

5.2.4. Технический контроль. Обеспечивает проверку эффективности защиты персональных данных с использованием технических и (или) программных средств контроля и в дальнейшем получение наиболее объективной и достоверной информации о состоянии объектов контроля.

6. Организационная структура и обязанности ответственных лиц

6.1. Приказом директора Центра назначается лицо, ответственное за обработку персональных данных (ответственное лицо), администратор информационной системы персональных данных (ИСПДн) и администратор безопасности ИСПДн, которые проводят мероприятия по защите персональных данных субъектов.

При необходимости дополнительно назначаются лица, ответственные за обработку персональных данных в учебных корпусах.

6.2. Доступ к персональным данным работников и обучающихся, воспитанников Центра имеют:

- директор;
- заместители директора (персональные данные работников, находящихся в их непосредственном подчинении, по направлению деятельности; персональные данные обучающихся, воспитанников по направлению деятельности);
- классные руководители (только к персональным данным обучающихся своего класса);
- воспитатели дошкольных групп (только к персональным данным воспитанников своей группы);
- иные работники, определяемые приказом директора Центра в пределах своей компетенции.

6.3. Помимо лиц, указанных в пункте 6.2. настоящего Положения, право доступа к персональным данным работников и обучающихся, воспитанников имеют только лица, уполномоченные действующим законодательством.

6.4. Лицо, ответственное за организацию обработки персональных данных:

6.4.1. Осуществляет внутренний контроль соблюдения требований по работе с персональными данными, в том числе требований к защите персональных данных.

6.4.2. Доводит до сведения работников, указанных в пункте 6.1, положения законодательства Российской Федерации о персональных данных, локальных нормативных актов по вопросам обработки персональных данных, требований к защите персональных данных.

6.4.3. Организует приём и обработку обращений и запросов субъектов персональных данных или их представителей и осуществляет контроль за приёмом и обработкой таких обращений и запросов.

6.5. Администратор ИСПДн отвечает за обеспечение работоспособности элементов ИСПДн и средств защиты персональных данных.

6.6. Администратор безопасности ИСПДн отвечает за обеспечение необходимого уровня состояния защиты ИСПДн, правильность настройки средств защиты, организацию выдачи, хранения и уничтожения материальных носителей персональных данных.

7. Обязанности Оператора и субъектов персональных данных

7.1. Оператор обязан использовать персональные данные только в соответствии с целями обработки, определившими их получение.

7.2. Сотрудники Центра обязаны не отвечать на запросы, связанные с передачей персональных данных, по телефону или факсу.

7.3. Для защиты персональных данных субъектов Оператор обязан:

7.3.1. За свой счёт, в порядке, установленном законодательством Российской Федерации, обеспечить защиту персональных данных субъекта от неправомерного их использования или утраты.

7.3.2. Ознакомить работника или его законного представителя с настоящим Положением под расписку.

7.3.3. По запросу ознакомить субъекта персональных данных, не являющегося сотрудником, или в случае недееспособности либо несовершеннолетия субъекта, его законного представителя с настоящим Положением под расписку.

7.3.4. Осуществлять передачу персональных данных субъекта только в соответствии с настоящим Положением и законодательством Российской Федерации.

7.3.5. Предоставлять персональные данные субъекта только уполномоченным лицам и только в той части, которая необходима им для выполнения их трудовых обязанностей в соответствии с настоящим Положением и законодательством Российской Федерации.

7.3.6. По требованию субъекта или его законного представителя предоставить ему полную информацию о его персональных данных и порядке обработки этих данных.

7.4. Субъект персональных данных или его законный представитель обязуется предоставлять персональные данные, соответствующие действительности.

8. Права субъектов персональных данных

Субъекты персональных данных имеют право:

8.1. На получение информации, касающейся обработки его персональных данных, в том числе содержащей:

8.1.1. Подтверждение факта обработки персональных данных оператором;

8.1.2. Правовые основания и цели обработки персональных данных;

8.1.3. Цели и применяемые оператором способы обработки персональных данных;

8.1.4. Наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

8.1.5. Обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

8.1.6. Сроки обработки персональных данных, в том числе сроки их хранения;

8.1.7. Порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ;

8.1.8. Информацию об осуществлённой или о предполагаемой трансграничной передаче данных;

8.1.9. Наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

8.1.10. Иные сведения, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ или другими федеральными законами.

8.2. Получать доступ к своим персональным данным, включая право получать копии любой записи, содержащей собственные персональные данные, за исключением случаев, предусмотренных федеральным законом.

8.3. Требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением законодательства.

При отказе Оператора или уполномоченного им лица исключить или исправить персональные данные субъекта – заявить в письменной форме о своём несогласии, представив соответствующее обоснование.

8.4. Требовать от Оператора уведомления всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта, обо всех произведённых в них изменениях.

8.5. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если:

8.5.1. Обработка персональных данных осуществляется в целях обороны страны, безопасности государства и охраны правопорядка.

8.5.2. Обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными.

8.5.3. Обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма.

8.5.4. Доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

8.5.5. Обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

9. Ответственность за нарушение норм, регулирующих получение, обработку и защиту персональных данных сотрудника

9.1. Директор Центра, разрешающий доступ сотрудника к конфиденциальному документу, содержащему персональные данные, несёт персональную ответственность за данное разрешение.

9.2. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, материальную, административную, уголовную ответственность, предусмотренную действующим законодательством Российской Федерации.

9.3. Каждый сотрудник несёт единоличную ответственность за сохранность и конфиденциальность полученных в процессе работы персональных данных субъектов.

9.4. За неисполнение или ненадлежащее исполнение сотрудником возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера директор Центра вправе применять предусмотренные Трудовым Кодексом дисциплинарные взыскания.

9.5. Должностные лица, в обязанность которых входит ведение персональных данных сотрудника, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации – влечёт наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.

10. Порядок доступа в помещения, в которых ведётся обработка персональных данных

10.1. Доступ в помещения, в которых происходит обработка персональных данных, осуществляется в рабочее время. В другое время нахождение в этих помещениях запрещается.

10.2. Работникам Центра не разрешается при любом по продолжительности выходе из помещения оставлять какие-либо документы, содержащие персональные данные на рабочем столе или оставлять шкафы (сейфы), в которых хранятся такие документы, незапертыми.

10.3. Работникам Центра запрещено покидать помещения, в которых ведётся обработка персональных данных, оставив там посторонних лиц. При отсутствии работников в кабинете, дверь в помещение должна быть заперта.

10.4. В конце рабочего дня на рабочем столе не должно оставаться документов с персональными данными.

10.5. По завершению работы все материальные носители, содержащие персональные данные, должны быть помещены в специально выделенные места хранения. Места хранения материальных носителей персональных данных определяются приказом директора Центра.

10.6. Уборка помещений допускается только в присутствии ответственных сотрудников.