МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ «ЦЕНТР ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ»

ПРИНЯТО:
Общим собранием
МБУ ДО «ЦДО»
Протокол № 3 от 24.09.2025

УТВЕРЖДЕНО:
Директор МБУ ДО ЦДО»
_____ Балеевских Н.П.
№01-03/157 от 24.09.2025

ПОЛОЖЕНИЕ ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ

1. Общие положения

1.1. Настоящее Положение определяет порядок обработки и защиты персональных данных работников муниципального бюджетного учреждения дополнительного образования «Центр дополнительного образования» (далее — Учреждение, Работодатель).

1.2. Положение разработано в соответствии с:

- Трудовым кодексом Российской Федерации;
- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (с изменениями, внесёнными Федеральным законом от 24.06.2025 № 156-ФЗ, от 28.12.2024 № 519-ФЗ, от 23.05.2025 № 121-ФЗ и иными нормативными правовыми актами);
- Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение обязанностей, возлагаемых на операторов персональных данных»;
- Приказом Роскомнадзора от 19.06.2025 № 140 «Об утверждении требований к методам обезличивания персональных данных»;
- иными нормативными правовыми актами Российской Федерации.

1.3. Положение устанавливает порядок обработки и защиты информации, содержащей сведения, отнесённые к персональным данным работников Учреждения, включая сбор, запись, систематизацию, накопление, хранение, уточнение, извлечение, использование, передачу, обезличивание, блокирование, удаление и уничтожение персональных данных.

1.4. Положение является локальным нормативным актом Учреждения, утверждается приказом директора Учреждения и действует в отношении всех работников Учреждения, а также лиц, прекративших трудовые отношения с Учреждением, в части хранения ранее полученных персональных данных.

1.5. Работодатель является оператором персональных данных. Уведомление о намерении осуществлять обработку персональных данных направлено в Роскомнадзор, Учреждение включено в реестр операторов персональных данных.

2. Цели и принципы обработки персональных данных

2.1. Обработка персональных данных работников Учреждения осуществляется в следующих целях:

- обеспечение соблюдения законодательства Российской Федерации, трудового законодательства;
- содействие работникам в трудоустройстве, обучении и продвижении по службе;
- обеспечение личной безопасности работников;
- контроль количества и качества выполняемой работы;
- обеспечение сохранности имущества Учреждения;
- ведение кадрового учёта и бухгалтерского расчёта;
- уплата налогов и страховых взносов;
- ведение воинского учёта;
- обеспечение пропускного режима в Учреждении.

2.2. Обработка персональных данных осуществляется с соблюдением следующих принципов:

- законность и справедливая основа обработки;
- ограничение обработки конкретными, заранее определёнными и законными целями;
- соответствие содержания и объёма обрабатываемых данных заявленным целям — избыточные данные не обрабатываются;
- обеспечение точности, достаточности, а в необходимых случаях и актуальности персональных данных;

- хранение персональных данных в форме, позволяющей определить субъекта, не дольше, чем этого требуют цели обработки, если срок хранения не установлен федеральным законом;
- уничтожение или обезличивание персональных данных по достижении целей обработки или при утрате необходимости в их достижении.

2.3. Не допускается:

- обработка персональных данных, несовместимая с целями их сбора;
- объединение баз данных, содержащих персональные данные, обработка которых осуществляется в несовместимых целях;
- избыточность обрабатываемых персональных данных по отношению к заявленным целям их обработки.

3. Состав персональных данных работников

3.1. В состав персональных данных, обрабатываемых Учреждением, входят:

Общие персональные данные:

- фамилия, имя, отчество;
- пол, дата и место рождения, возраст;
- гражданство;
- паспортные данные;
- адрес регистрации по месту жительства (месту пребывания) и адрес фактического проживания;
- идентификационный номер налогоплательщика (ИНН);
- страховой номер индивидуального лицевого счёта (СНИЛС);
- сведения об образовании, квалификации, профессиональной подготовке, повышении квалификации;
- сведения о трудовой деятельности (место работы, период, стаж);
- сведения о семейном положении, составе семьи (степень родства, ФИО, даты рождения);
- реквизиты свидетельств о государственной регистрации актов гражданского состояния;
- сведения о доходах, обязательствах по исполнительным документам;
- номера расчетного счёта, банковской карты;
- сведения о воинском учёте;
- фотографии работников;
- контактные данные (телефон, адрес электронной почты).

Специальные категории персональных данных (обрабатываются только в случаях, прямо предусмотренных законом):

- сведения о состоянии здоровья (в объёме, необходимом для решения вопроса о возможности выполнения трудовых функций);
- сведения о судимости (в случаях, предусмотренных законодательством для работы с несовершеннолетними).

Биометриеские персональные данные (обрабатываются с письменного согласия работника):

- фотографии, используемые для установления личности при пропускном режиме (если применимо в Учреждении).

3.2. Работодатель не вправе требовать от работника представления персональных данных, которые не характеризуют работника как сторону трудовых отношений.

4. Получение персональных данных

4.1. Персональные данные работника Работодатель получает непосредственно от работника. Работодатель вправе получать персональные данные работника от третьих лиц только при наличии письменного согласия работника или в иных случаях, прямо предусмотренных законодательством.

4.2. Работодатель обязан сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.
4.3. Работник представляет Работодателю достоверные сведения о себе. Работодатель проверяет достоверность сведений, сверяя данные, представленные работником, с имеющимися у него документами.
4.4. Обработка персональных данных работников осуществляется как с использованием средств автоматизации (информационные системы, электронные базы данных), так и без использования средств автоматизации (на бумажных носителях).

5. Согласие на обработку персональных данных
5.1. Обработка персональных данных работников осуществляется на следующих правовых основаниях:
- исполнение трудового законодательства, трудового договора;
- исполнение иных обязанностей, возложенных на Работодателя законом (налоговое законодательство, пенсионное, воинский учёт и др.) — согласие работника не требуется;
- в случаях, не покрываемых законным основанием, — на основании отдельного согласия работника.

5.2. В соответствии с требованиями Федерального закона № 152-ФЗ (в редакции Федерального закона от 24.06.2025 № 156-ФЗ) согласие на обработку персональных данных оформляется исключительно в виде отдельного документа. Включение согласия в текст трудового договора, заявления, анкеты или иного документа не допускается.
5.3. Согласие на обработку персональных данных должно быть конкретным, предметным, информированным, сознательным и однозначным.
5.4. Согласие на обработку персональных данных, разрешённых для распространения, оформляется отдельно от иных согласий на обработку персональных данных работника.
5.5. В согласии в обязательном порядке указываются:
- фамилия, имя, отчество и адрес субъекта персональных данных;
- наименование и адрес оператора (Учреждения);
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых даётся согласие;
- перечень действий с персональными данными, на совершение которых даётся согласие;
- срок действия согласия и способ его отзыва.

5.6. Согласие оформляется на бумажном носителе с собственноручной подписью работника либо в форме электронного документа, подписанного усиленной квалифицированной электронной подписью.
5.7. Работник вправе отозвать согласие в любое время. Отзыв согласия не прекращает обработку персональных данных, осуществляемую на основании закона (исполнение трудового законодательства, налоговых обязанностей и т.д.), но прекращает обработку, единственным основанием которой было это согласие.
5.8. Согласия, полученные до 1 сентября 2025 года в составе трудовых договоров или иных документов, продолжают действовать; переоформлять их не требуется. Новые согласия оформляются в соответствии с требованиями пункта 5.2 настоящего Положения.

6. Передача и распространение персональных данных
6.1. При передаче персональных данных работника Работодатель обязан соблюдать следующие требования:
- не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо для предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных Трудовым кодексом РФ или иными федеральными законами;

- не сообщать персональные данные работника в коммерческих целях без письменного согласия работника;
- лицам, получающим персональные данные работника, сообщать о необходимости соблюдения режима конфиденциальности.

6.2. Передача персональных данных без согласия работника допускается в следующих случаях:

- по запросу государственных органов в порядке, установленном законодательством (ФНС, СФР, органы прокуратуры, органы государственного надзора за соблюдением трудового законодательства и др.);
- в целях предупреждения угрозы жизни и здоровью работника;
- в иных случаях, прямо предусмотренных федеральным законом.

6.3. Лицо, обратившееся с запросом и не уполномоченное федеральным законом на получение информации, содержащей персональные данные работника, получает отказ в выдаче информации. Копия уведомления об отказе подшивается в личное дело работника.
6.4. Передача персональных данных работников по телефону запрещается в связи с невозможностью идентификации лица, запрашивающего информацию.
6.5. При передаче персональных данных работника подрядчику, осуществляющему обработку по поручению Работодателя, договор с подрядчиком должен содержать:

- перечень передаваемых данных;
- перечень и описание операций, которые поручается выполнить;
- цели обработки;
- обязательства подрядчика по обеспечению конфиденциальности и безопасности;
- требования к защите персональных данных.

6.6. Трансграничная передача персональных данных работников Учреждения не осуществляется. В случае возникновения такой необходимости Работодатель предварительно уведомляет Роскомнадзор в установленном порядке.

7. Локализация персональных данных

7.1. В соответствии с ч. 5 ст. 18 Федерального закона № 152-ФЗ (с 1 июля 2025 года) первичный сбор, запись, систематизация, накопление и хранение персональных данных граждан Российской Федерации осуществляются исключительно на территории Российской Федерации.
7.2. Учреждение не использует зарубежные серверы, базы данных, облачные хранилища и учётные системы для первичного накопления и хранения персональных данных работников.
7.3. В случае использования программного обеспечения, размещённого на зарубежных серверах, Учреждение обеспечивает передачу данных только после их первичной локализации на территории Российской Федерации через API или иные способы, не предполагающие первичное накопление данных за рубежом.

8. Доступ к персональным данным работников

8.1. Право доступа к персональным данным работников имеют:

- директор Учреждения;
- заместитель директора;
- специалист по кадрам;
- главный бухгалтер / бухгалтер;
- специалист по охране труда;
- иные работники, допущенные приказом директора Учреждения в пределах, необходимых для выполнения должностных обязанностей.

8.2. Доступ к персональным данным предоставляется на основании приказа директора Учреждения с указанием конкретного перечня доступных данных и допустимых операций.

8.3. Все работники, допущенные к обработке персональных данных, подписывают обязательство о неразглашении персональных данных. Без подписания указанного обязательства работник к обработке персональных данных не допускается.
8.4. Доступ предоставляется по принципу минимальной необходимости:

- специалист по кадрам имеет доступ к личным делам работников;
- бухгалтер имеет доступ к данным, необходимым для расчёта заработной платы и отчётности (ИНН, СНИЛС, банковские реквизиты, сведения о доходах, удержаниях);
- руководитель структурного подразделения имеет доступ только к сведениям, необходимым для управления;
- специалист по охране труда имеет доступ к сведениям о состоянии здоровья, необходимым для обеспечения безопасности.

8.5. Доступ пересматривается при переводе работника на другую должность или увольнении. При увольнении работника, имевшего доступ к персональным данным, доступ закрывается в день увольнения.
8.6. Использование общих сетевых папок, пересылка личных документов работников через мессенджеры и бессрочные выгрузки персональных данных на рабочие столы запрещены.

9. Хранение персональных данных
9.1. Персональные данные работников, обрабатываемые без использования средств автоматизации, хранятся на бумажных носителях в отделе кадров Учреждения в запирающихся шкафах или сейфах. Доступ к шкафам и сейфам имеют только уполномоченные работники.
9.2. Документы, содержащие персональные данные, хранятся обособленно от иной информации, если цели их обработки несовместимы.
9.3. Персональные данные, обрабатываемые с использованием средств автоматизации, хранятся в информационной системе персональных данных (ИСПДн) Учреждения на серверах, физически расположенных на территории Российской Федерации.
9.4. Сроки хранения персональных данных определяются целями обработки, требованиями законодательства и архивными правилами:

Категория данных	Срок хранения	Основание
Личные дела работников	75 лет (до 2003 года) / 50 лет (с 2003 года)	Архивный закон, Приказ Росархива
Трудовые договоры	75 лет / 50 лет	Архивный закон
Документы по бухгалтерскому учёту (зарплата)	5 лет	Закон о бухгалтерском учёте
Резюме кандидатов, не принятых на работу	до 6 месяцев	Цель обработки достигнута
Согласия на обработку ПД	До отзыва согласия или истечения срока	ФЗ-152
Документы воинского учёта	В соответствии с законодательством о воинском учёте	ФЗ «О воинской обязанности и военной службе»

9.5. При достижении целей обработки или утрате необходимости в их достижении персональные данные подлежат уничтожению или обезличиванию, если федеральным законом не установлено иное.

10. Защита персональных данных
10.1. Работодатель обеспечивает безопасность персональных данных при их обработке в информационных системах и без использования средств автоматизации.

Организационные меры защиты:

- назначение ответственного за обработку персональных данных приказом директора Учреждения;
- ограничение доступа к персональным данным (см. раздел 8);
- учёт и хранение носителей персональных данных в защищённых помещениях;
- ведение журнала выдачи и возврата документов, содержащих персональные данные;
- ознакомление работников под роспись с настоящим Положением и обязательствами о неразглашении;
- обучение работников, допущенных к обработке персональных данных.

Технические меры защиты (для ИСПДн):

- использование антивирусного программного обеспечения;
- применение парольной защиты учётных записей;
- ограничение прав доступа пользователей в информационной системе;
- обеспечение резервного копирования данных;
- регистрация и учёт действий пользователей в системе;
- использование сертифицированных средств защиты информации (при необходимости).

Меры защиты при неавтоматизированной обработке:

- хранение документов в запирающихся шкафах и сейфах;
- обеспечение режима безопасности помещений, в которых хранятся документы;
- запрет на оставление документов с персональными данными в доступных местах;
- запрет на использование оборотной стороны документов с персональными данными в качестве черновиков.

10.2. Работодатель не несёт ответственности за нарушение положений о защите персональных данных (статья 3.18.), совершённое работником, если Работодатель принял все необходимые меры по обеспечению защиты персональных данных.

11. Обезличивание персональных данных

11.1. В соответствии с Федеральным законом от 08.08.2024 № 233-ФЗ и Приказом Роскомнадзора от 19.06.2025 № 140 Учреждение вправе осуществлять обезличивание персональных данных для предоставления обезличенной информации в государственную информационную систему (ГИС) по требованию Минцифры России.

11.2. Обезличивание осуществляется утверждёнными методами, обеспечивающими невозможность восстановления персональных данных без дополнительной информации.

11.3. Обезличенные персональные данные могут быть использованы для статистических и аналитических целей без согласия субъекта персональных данных.

12. Реагирование на инциденты безопасности

12.1. При выявлении факта несанкционированного доступа к персональным данным, их утечки или угрозы такой утечки ответственный за обработку персональных данных немедленно информирует директора Учреждения.

12.2. Работодатель обязан уведомить Роскомнадзор о факте утечки персональных данных в течение 24 часов с момента выявления инцидента.

12.3. Уведомление должно содержать:

- обстоятельства инцидента;
- состав персональных данных, затронутых инцидентом;
- количество субъектов персональных данных, затронутых инцидентом;
- принятые меры по устранению последствий инцидента.

12.4. Работодатель принимает незамедлительные меры по локализации инцидента, восстановлению защиты персональных данных и предупреждению повторных инцидентов.

13. Права работников в области персональных данных

13.1. Работник имеет право на:

- получение информации, касающейся обработки его персональных данных, в том числе: целей обработки, категории обрабатываемых данных, сроков хранения, способов обработки;
- доступ к своим персональным данным, включая право на получение копии;
- требование уточнения, блокирования или уничтожения своих персональных данных в случае, если они являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- отзыв согласия на обработку персональных данных;
- обжалование действий или бездействия Работодателя в уполномоченный государственный орган по защите прав субъектов персональных данных (Роскомнадзор) или в судебном порядке.

13.2. Работник вправе осуществлять свои права лично или через представителя, полномочия которого оформлены в установленном законом порядке.
13.3. Работодатель обязан рассмотреть обращение работника по вопросам обработки его персональных данных и предоставить мотивированный ответ в срок, не превышающий 30 дней с даты обращения.

14. Ответственность за нарушение требований по обработке персональных данных
14.1. Работники Учреждения, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут ответственность в соответствии с:

- дисциплинарной — в порядке, установленном Трудовым кодексом РФ (замечание, выговор, увольнение);
- гражданско-правовой — в порядке, установленном гражданским законодательством;
- административной — по статье 13.11 КоАП РФ;
- уголовной — по статье 137 УК РФ при наличии состава преступления.

14.2. В соответствии с действующей редакцией статьи 13.11 КоАП РФ (в редакции Федерального закона от 30.11.2024 № 420-ФЗ) за нарушение требований к обработке персональных данных предусмотрены следующие размеры административной ответственности:

- обработка персональных данных без согласия субъекта: для юридических лиц — от 150 000 до 300 000 руб., при повторном нарушении — от 300 000 до 1 500 000 руб.;
- утечка персональных данных: от 60 000 до 15 000 000 руб. в зависимости от количества затронутых субъектов и категории данных;
- утечка биометрических данных: для юридических лиц — от 15 000 000 до 20 000 000 руб.;
- неуведомление Роскомнадзора об утечке: для юридических лиц — от 1 000 000 до 3 000 000 руб.;
- нарушение требований локализации: от 1 000 000 до 6 000 000 руб., при повторном нарушении — от 6 000 000 до 18 000 000 руб.

14.3. При повторном нарушении, повлекшем утечку персональных данных, может быть применён оборотный штраф в размере от 1% до 3% годовой выручки, но не менее 20 000 000 руб. и не более 500 000 000 руб.

15. Уничтожение персональных данных
15.1. Уничтожение персональных данных производится в следующих случаях:

- достижение целей обработки персональных данных;
- утрата необходимости в достижении целей обработки;
- истечение срока хранения, установленного законодательством или настоящим Положением;
- отзыв согласия работника (в части обработки, основанной исключительно на согласии);

- ликвидация Учреждения.

15.2. Уничтожение персональных данных, обрабатываемых с использованием средств автоматизации, включает:

- удаление записей из информационной системы;
- удаление резервных копий по принятому циклу резервирования;
- удаление временных выгрузок и файлов, содержащих персональные данные.

15.3. Уничтожение персональных данных, обрабатываемых без использования средств автоматизации, производится путём:

- сжигания бумажных носителей;
- измельчения бумажных носителей с помощью шредера до степени, исключающей восстановление текста.

15.4. Результат уничтожения персональных данных оформляется актом об уничтожении персональных данных, подписываемым комиссией, назначенной приказом директора Учреждения.

16. Заключительные положения

16.1. Настоящее Положение вступает в силу с момента его утверждения приказом директора Учреждения.

16.2. Все работники Учреждения должны быть ознакомлены с настоящим Положением под роспись в срок, не превышающий 5 рабочих дней с даты его утверждения.

16.3. Внесение изменений в настоящее Положение осуществляется приказом директора Учреждения. Работники знакомятся с изменениями под роспись в течение 5 рабочих дней с даты издания приказа о внесении изменений.

16.4. В случае изменения законодательства Российской Федерации о персональных данных настоящее Положение подлежит приведению в соответствие с изменёнными нормами в течение 30 календарных дней с даты вступления изменений в силу.

16.5. Настоящее Положение хранится в отделе кадров Учреждения, а также размещается на информационном стенде и (или) официальном сайте Учреждения.