СОГЛАСОВАНО
Председателем первичной
профсоюзной организации
МБУДО ЦТ «Калейдоскоп»
_____ Ю.А. Шашина
«10» июня 2026 г.

УТВЕРЖДЕНО
приказом МБУДО ЦТ «Калейдоскоп»
от 10 июня 2026 № 159

МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ ЦЕНТР ТВОРЧЕСТВА "КАЛЕЙДОСКОП" МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ ТИМАШЕВСКИЙ МУНИЦИПАЛЬНЫЙ РАЙОН КРАСНОДАРСКОГО КРАЯ

Подписано цифровой подписью: МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ ЦЕНТР ТВОРЧЕСТВА "КАЛЕЙДОСКОП" МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ ТИМАШЕВСКИЙ МУНИЦИПАЛЬНЫЙ РАЙОН КРАСНОДАРСКОГО КРАЯ

ПОЛОЖЕНИЕ
о защите персональных данных МБУДО ЦТ «Калейдоскоп»

1. Общие положения

1.1. Положение о защите персональных данных муниципального бюджетного учреждения дополнительного образования Центр творчества «Калейдоскоп» муниципального образования Тимашевский муниципальный район Краснодарского края (далее – Учреждение) разработано в соответствии с Трудовым кодексом РФ, Федеральным законом от 27.07.2006 № 152-ФЗ, нормативными правовыми актами в области защиты персональных данных, действующими на территории России (далее — Положение).

1.2. Цель настоящего Положения – защита персональных данных работников, учащихся и их родителей (законных представителей) Учреждения от несанкционированного доступа и разглашения, предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений.

1.3. Основные понятия:

- **персональные данные (далее – ПД)** – любая информация, прямо или косвенно относящаяся к субъекту персональных данных;
- **угроза безопасности ПД** – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных;
- **уровень защищенности ПД** – комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности ПД при их обработке в информационной системе.

1.4. Настоящее Положение распространяется на работников Учреждения. Все работники должны быть ознакомлены под подпись с данным Положением и изменениями к нему.

1.5. Настоящее Положение вступает в силу со дня его утверждения приказом директора Учреждения и согласования с профсоюзным органом Учреждения и действует бессрочно до принятия нового положения.

2. Меры по обеспечению безопасности персональных данных

2.1. Организационные меры:

назначение лица, ответственного за обработку ПД, которое осуществляет организацию обработки ПД, внутренний контроль за соблюдением работниками требований к защите ПД;

разработка и утверждение внутренних документов по обработке и защите ПД;

регламентация доступа сотрудников к ПД в зависимости от их должностных обязанностей;

организация пропускного режима и контроля доступа в помещения, где осуществляется обработка ПД;

осуществление внутреннего контроля и аудита.

2.2. Технические меры:

разграничение прав доступа к информационным системам, обрабатывающим ПД;

установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их трудовыми обязанностями;

применение средств криптографической защиты при передаче ПД по сетям связи;

своевременное обновление программного обеспечения.

2.3. Физические меры:

использование запираемых шкафов и сейфов для хранения бумажных носителей ПД;

утилизация носителей ПД с соблюдением требований по защите информации;

соблюдение условий, обеспечивающих сохранность ПД и исключающих несанкционированный к ним доступ;

обнаружение фактов несанкционированного доступа к ПД;

восстановление ПД, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

определение типа угроз безопасности и уровней защищенности ПД, которые хранятся в информационных системах.

3. Угрозы защищенности персональных данных

3.1. Угрозы первого типа. В системном программном обеспечении информационной системы есть функциональные возможности программного обеспечения, которые не указаны в описании к нему либо не отвечают характеристикам, которые заявил производитель. И это потенциально может привести к неправомерному использованию ПД.

3.2. Угрозы второго типа. Потенциальные проблемы с прикладным программным обеспечением — внешними программами, которые установлены на компьютерах работников.

3.3. Угрозы третьего типа. Потенциальной опасности ни от системного, ни от программного обеспечения нет.

4. Уровни защищенности персональных данных

4.1. Виды уровней защищенности ПД:

Первый уровень защищенности. Если комиссия по защите ПД отнесла информационную систему к первому типу угрозы или если тип угрозы второй, но Учреждение обрабатывает специальные категории ПД более 100 тыс. физических лиц без учета сотрудников.

Второй уровень защищенности. Если тип угрозы второй и Учреждение обрабатывает биометрические и специальные категории ПД сотрудников вне зависимости от их количества или специальные категории ПД менее чем 100 тыс. физических лиц, или любые другие категории ПД более чем 100 тыс. физических лиц, или при третьем типе угрозы Учреждение обрабатывает специальные категории данных более чем 100 тыс. физических лиц.

Третий уровень защищенности. Если при втором типе угрозы Учреждение обрабатывает общие ПД сотрудников или менее чем 100 тыс. физических лиц, или при третьем типе угрозы Учреждение обрабатывает специальные категории ПД сотрудников или менее чем 100 тыс. физических лиц, или при третьем типе угрозы Учреждение обрабатывает биометрические ПД, или при третьем типе угрозы Учреждение обрабатывает общие ПД более чем 100 тыс. физических лиц.

Четвертый уровень защищенности. Если при третьем типе угрозы работодатель обрабатывает только общие ПД сотрудников или менее чем 100 тыс. физических лиц.

4.2. При четвертом уровне защищенности ПД Учреждение:

- обеспечивает режим безопасности помещений, в которых размещаете информационную систему;
- обеспечивает сохранность носителей информации;
- утверждает перечень работников, допущенных к работе с ПД;
- использует средства защиты информации, которые прошли оценку соответствия требованиям закона в области обеспечения безопасности информации.

4.3. При третьем уровне защищенности ПД дополнительно к мерам, перечисленным в пункте 4.2. настоящего Положения, Учреждение назначает ответственного за обеспечение безопасности ПД в информационной системе.

4.4. При втором уровне защищенности ПД дополнительно к мерам, перечисленным в пунктах 4.2,4.3, настоящего Положения, Учреждение ограничивает доступ к электронному журналу сообщений, за исключением работников, которым такие сведения необходимы для работы.

4.5. При первом уровне защищенности ПД дополнительно к мерам, перечисленным в пунктах 4.2 – 4.4 настоящего Положения, Учреждение:

- обеспечивает автоматическую регистрацию в электронном журнале безопасности изменения полномочий работников по допуску к ПД в системе;
- создает отдел, ответственный за безопасность ПД в системе, либо возлагает такую обязанность на один из существующих отделов работодателя.

4.6. В целях защиты ПД на бумажных носителях Учреждение:

- приказом назначает ответственного за обработку ПД;
- ограничивает допуск в помещения, где хранятся документы, которые содержат ПД субъектов;
- хранит документы, содержащие ПД субъектов, в шкафах, запирающихся на ключ;
- хранит трудовые и медицинские книжки сотрудников в сейфе у директора Учреждения.

4.7. В целях обеспечения конфиденциальности документы, содержащие ПД субъектов, оформляются, ведутся и хранятся следующими сотрудниками:

бухгалтер;

специалист по кадрам;

заместители директора;

методисты;

педагоги дополнительного образования.

4.8. Сотрудники, допущенные к ПД субъектов, подписывают обязательства о неразглашении ПД и соглашение о неразглашении ПД. В противном случае до обработки ПД сотрудников не допускают.

4.9. Передача ПД по запросам третьих лиц, если такая передача прямо не предусмотрена законодательством РФ, допускается исключительно с согласия субъекта на обработку его ПД в части их предоставления или согласия на распространение ПД.

4.10. Передача информации, содержащей сведения о ПД субъектов, по телефону в связи с невозможностью идентификации лица, запрашивающего информацию, запрещается.

5. Цели обработки персональных данных

5.1. Учреждение может обрабатывать ПД субъектов в следующих случаях:

5.1.1. От субъекта получено согласие на обработку его ПД;

5.1.2. Учреждение выполняет обязанности, которые на него возложены законодательством Российской Федерации;

5.1.3. В связи с участием в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах, а также для исполнения судебного акта, акта другого органа или должностного лица в соответствии с законодательством Российской Федерации об исполнительном производстве;

5.1.4. Для защиты жизни, здоровья или иных жизненно важных интересов субъекта, если невозможно получить его согласие.

5.2. Учреждение обрабатывает персональные данные в следующих целях:

5.2.1. Ведение кадрового и бухгалтерского учета.

В рамках указанной цели обрабатываются следующие ПД сотрудников: фамилия, имя, отчество; дата, месяц, год рождения; семейное положение; пол; гражданство; адрес регистрации и места жительства; данные документа, удостоверяющего личность; СНИЛС; ИНН; доходы; номер расчетного счета; реквизиты банковской карты; профессия; должность; сведения о трудовой

деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время с указанием наименования и расчетного счета организации).

Обрабатываемые в рамках указанной цели ПД не относятся к специальным категориям или биометрическим.

ПД обрабатываются с использованием средств автоматизации и без использования таких средств.

ПД обрабатываются в период действия трудового договора с сотрудником. Документы с ПД хранятся в течение срока, установленного законодательством РФ. Срок хранения ПД в информационных системах соответствует сроку хранения аналогичных бумажных документов с ПД.

Персональные данные подлежат уничтожению по окончании срока хранения документов, которые содержат ПД, в порядке, предусмотренном настоящим Положением.

5.2.2. Обеспечение соблюдения трудового законодательства.

В рамках указанной цели обрабатываются следующие ПД работников, не относящиеся к специальным категориям или биометрическим: фамилия, имя, отчество; дата, месяц, год рождения; семейное положение; пол; гражданство; адрес регистрации и места жительства; данные документа, удостоверяющего личность; адрес электронной почты; номер телефона; СНИЛС; ИНН; доходы; номер расчетного счета; реквизиты банковской карты; данные водительского удостоверения; профессия; должность; сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время с указанием наименования и расчетного счета организации); отношение к воинской обязанности, сведения о воинском учете; сведения об образовании; сведения о состоянии здоровья.

В рамках указанной цели обрабатываются следующие ПД сотрудников – специальные категории ПД: сведения о состоянии здоровья.

В рамках указанной цели могут обрабатываться следующие ПД родственников работников, не относящиеся к специальным категориям или биометрическим: фамилия, имя, отчество; дата, месяц, год рождения; семейное положение; адрес регистрации и места жительства; данные документа, удостоверяющего личность; адрес электронной почты; номер телефона; должность; сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время с указанием наименования организации); отношение к воинской обязанности, сведения о воинском учете; сведения об образовании.

ПД обрабатываются с использованием средств автоматизации и без использования таких средств.

ПД обрабатываются в период действия трудового договора с сотрудником. Документы с ПД хранятся в течение срока, установленного законодательством РФ. Срок хранения ПД в информационных системах соответствует сроку хранения аналогичных бумажных документов с ПД.

Персональные данные подлежат уничтожению по окончании срока хранения документов, которые содержат ПД, в порядке, предусмотренном настоящим Положением.

5.2.3. Обеспечение соблюдения налогового законодательства.

В рамках указанной цели обрабатываются следующие ПД работников: фамилия, имя, отчество; дата, месяц, год рождения; семейное положение; пол; гражданство; адрес регистрации и места жительства; данные документа, удостоверяющего личность; СНИЛС; ИНН; доходы; номер расчетного счета; реквизиты банковской карты; должность; сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время с указанием наименования и расчетного счета организации).

Обрабатываемые в рамках указанной цели ПД не относятся к специальным категориям или биометрическим.

ПД обрабатываются с использованием средств автоматизации и без использования таких средств.

ПД обрабатываются в период действия трудового договора с сотрудником. Документы с ПД хранятся в течение срока, установленного законодательством РФ. Срок хранения ПД в информационных системах соответствует сроку хранения аналогичных бумажных документов с ПД.

Персональные данные подлежат уничтожению по окончании срока хранения документов, которые содержат ПД, в порядке, предусмотренном настоящим Положением.

5.2.4. Подбор персонала на вакантные должности.

В рамках указанной цели обрабатываются следующие ПД соискателей: фамилия, имя, отчество; дата, месяц, год рождения; гражданство; адрес регистрации; адрес электронной почты; номер телефона; профессия; должность; сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время с указанием наименования и расчетного счета организации); сведения об образовании.

Обрабатываемые в рамках указанной цели ПД не относятся к специальным категориям или биометрическим.

ПД обрабатываются с использованием средств автоматизации и без использования таких средств.

ПД обрабатываются в течение периода принятия решения о трудоустройстве.

ПД подлежат уничтожению в течение 30 дней с момента принятия решения об отказе в трудоустройстве в порядке, предусмотренном настоящим Положением.

5.2.5. Организация образовательного процесса и учебно-воспитательной деятельности.

В рамках указанной цели обрабатываются следующие ПД учащихся и их родителей (законных представителей): фамилия, имя, отчество (последнее – при наличии); дата, месяц, год рождения учащегося; пол; гражданство; адрес регистрации и места жительства; данные документа, удостоверяющего личность; СНИЛС; фамилия, имя, отчество (последнее – при наличии) родителя (законного представителя); данные документа, удостоверяющего личность родителя (законного представителя), адрес электронной почты, телефон; сведения о состоянии здоровья учащегося.

В рамках указанной цели обрабатываются следующие ПД учащегося – специальные категории ПД: сведения о состоянии здоровья.

ПД обрабатываются с использованием средств автоматизации и без использования таких средств.

ПД обрабатываются в период действия оказания образовательной услуги учащемуся.

Персональные данные подлежат уничтожению по окончании срока хранения документов, которые содержат ПД, в порядке, предусмотренном настоящим Положением.

6. Права и обязанности субъектов ПД

6.1. Субъект ПД имеет право на:

- доступ к своим ПД, включая право на получение копий любой записи, содержащей ПД, за исключением случаев, предусмотренных федеральным законом;
- уточнение своих ПД, их блокирование или уничтожение в случае, если ПД являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- отзыв согласия на обработку ПД. Для этого субъект должен направить в Учреждение в письменной форме отзыв согласия. В случае отзыва согласия на обработку ПД Учреждение вправе продолжить обработку ПД без согласия Работника при наличии оснований, предусмотренных пунктами 5.1.2–5.1.4 настоящего Положения;
- требование прекратить передачу (распространение, предоставление, доступ) своих персональных данных, ранее разрешенных для распространения.

6.2. Субъект ПД обязан:

- предоставлять Учреждению достоверные персональные данные;
- сообщать Учреждению об изменении своих ПД в течение 3 рабочих дней со дня наступления соответствующих изменений.

7. Обязанности Учреждения

7.1. Учреждение обязано:

- принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПД от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении ПД;
- не сообщать ПД субъекта третьим лицам без его письменного согласия, за исключением случаев, предусмотренных федеральными законами;
- разрешать доступ к ПД субъектов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те ПД, которые необходимы для выполнения конкретных трудовых обязанностей;
- предоставлять субъекту ПД по его просьбе информацию, касающуюся обработки его ПД;

- прекратить передачу (распространение, предоставление, доступ) персональных данных, прекратить обработку и уничтожить персональные данные в порядке и случаях, предусмотренных федеральными законами;

8. Обязанности лиц, допущенных к обработке ПД

Лица, осуществляющие обработку ПД сотрудников, учащихся и их родителей (законных представителей), обязаны:

- не разглашать третьим лицам ПД, которые известны ему в связи с исполнением трудовых обязанностей;
- не использовать ПД с целью получения личной выгоды;
- выполнять требования законодательства РФ в области ПД и локальных нормативных актов Учреждения, регламентирующих порядок обработки ПД;
- докладывать директору Учреждения обо всех фактах и попытках несанкционированного доступа к ПД и утечке ПД;
- после прекращения прав на допуск к ПД (перевод на другую должность, увольнение) не разглашать и не передавать ПД третьим лицам и не уполномоченным на это сотрудникам в течение 3 лет;
- все материальные (бумажные и электронные) носители ПД при увольнении передать директору Учреждения.

В случае разглашения ПД сотрудник может быть привлечен к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом РФ и иными федеральными законами. Кроме того, он может быть привлечен к административной, гражданско-правовой или уголовной ответственности в порядке, установленном федеральными законами.

9. Уничтожение персональных данных

9.1. Для уничтожения документов, которые содержат ПД, создается комиссия по уничтожению данных. Комиссия составляет список с указанием документов, иных материальных носителей и (или) сведений в информационных системах, содержащих персональные данные, которые подлежат уничтожению.

9.2. Бумажные носители информации уничтожаются путем сжигания. Документом, подтверждающим уничтожение ПД, является акт об уничтожении ПД.

9.3. ПД, которые хранятся в информационных системах, удаляются из этих систем. Документом, подтверждающим удаление ПД, является акт об уничтожении персональных данных и выгрузка из журнала регистрации событий в информационной системе персональных данных.

10. Заключительные положения

10.1. Настоящее Положение вступает в силу с момента его утверждения приказом директора Учреждения и согласования с профсоюзным органом Учреждения.

10.2. Изменения и дополнения в Положение вносятся в порядке, предусмотренном для его утверждения.

10.3. Контроль за соблюдением Положения возлагается на ответственного за организацию обработки персональных данных.

10.4. Положение действует бессрочно до принятия нового документа взамен настоящего.