

**МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ  
ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ  
«КРАСНОЯРУЖСКАЯ ДЕТСКО-ЮНОШЕСКАЯ СПОРТИВНАЯ ШКОЛА»**

ПРИНЯТО

На заседании педагогического совета.  
Протокол № 6 от «06» июня 2023 г.

УТВЕРЖДЕНО

Приказ № 103 от «06» июня 2023 г.

**ПОЛОЖЕНИЕ  
ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ,  
ОБУЧАЮЩИХСЯ И ИХ РОДИТЕЛЕЙ (ЗАКОННЫХ ПРЕДСТАВИТЕЛЕЙ)**

**1. Общие положения**

1.1. Настоящее положение (далее – Положение) разработано в соответствии со ст. 18.1 Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных» (далее – Закон о персональных данных) и является основополагающим локальным нормативным актом МБУДО «Краснояржская ДЮСШ» (далее - Учреждение), определяющим ключевые направления деятельности в области обработки и защиты персональных данных, оператором которого является Учреждение.

1.2. Положение разработано в целях реализации требований законодательства в области обработки и защиты персональных данных и направлено на обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, частной и семейной тайн.

1.3. Действие Положения распространяется на отношения по обработке и защите персональных данных, полученных Учреждением как до, так и после утверждения Положения, за исключением случаев, когда по причинам правового, организованного и иного характера требования Положения не могут быть распространены на отношения по обработке и защите персональных данных, полученных до ее утверждения.

1.4. Если в отношениях с Учреждением участвуют наследники (правопреемники) и (или) представители субъектов персональных данных, то Учреждение становится оператором персональных данных лиц, представляющих указанных субъектов. Положение и другие внутренние регулятивные документы школы распространяются на случаи обработки и защиты персональных данных наследников (правопреемников) и (или) представителей субъектов персональных данных, даже если эти лица в локальных нормативных актах прямо не упоминаются, но фактически участвуют в правоотношениях с Учреждением.

**2. Понятие и состав персональных данных.**

2.1. Персональные данные – информация, необходимая Учреждению в связи с осуществлением образовательной деятельности и трудовыми отношениями (в том числе полученная посредством информационных систем в сети «Интернет»).

2.2. Состав персональных данных работников, обучающихся и их родителей (законных представителей):

- фамилия, имя, отчество;
- дата рождения;
- образование;
- данные свидетельства о рождении обучающегося;
- СНИЛС;
- сведения о трудовом стаже;
- сведения о составе семьи;

- паспортные данные;
- сведения о воинском учете;
- сведения о заработной плате сотрудника;
- сведения о социальных льготах;
- специальность, квалификация;
- занимаемая должность;
- наличие судимостей;
- адрес регистрации и места жительства;
- контактный телефон;
- место работы или учебы членов семьи и родственников;
- сведения о семейном положении;
- содержание трудового договора;
- сведения о повышении квалификации, переподготовке и аттестации.

### **3. Обязанности работодателя.**

3.1. В целях обеспечения прав и свобод работников, обучающихся и их родителей (законных представителей) Учреждение и его представители при обработке персональных данных работника обязаны соблюдать следующие общие требования:

3.1.1. Обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам, обучающимся и их родителям (законным представителям)

3.1.2. При определении объема и содержания, обрабатываемых персональных данных Учреждение должно руководствоваться Конституцией Российской Федерации, Трудовым кодексом и иными федеральными законами.

3.1.3. При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения.

3.1.4. Защита персональных данных от неправомерного их использования или утраты должна быть обеспечена Учреждением за счет его средств в порядке, установленном федеральным законом.

3.1.5. Работники и их представители должны быть ознакомлены под расписку с документами организации, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

3.1.6. Участники образовательного процесса не должны отказываться от своих прав на сохранение и защиту тайны.

### **4. Обязанности субъекта персональных данных.**

4.1. Передавать Учреждению или его полномочному должностному лицу комплекс достоверных, документированных персональных данных, состав которых установлен настоящим Положением.

4.2. Своевременно сообщать Учреждению об изменении своих персональных данных.

### **5. Права субъекта персональных данных.**

5.1. Требовать исключения или исправления неверных или неполных персональных данных.

5.2. Право на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные.

5.3. Персональные данные оценочного характера дополнить заявлением, выражающим его собственную точку зрения.

5.4. Определять своих представителей для защиты своих персональных данных.

5.5. На сохранение и защиту своей личной и семейной тайны и персональных данных.

5.6. В случае когда обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, заключаемый с субъектом персональных данных договор не может содержать положения, ограничивающие права и свободы субъекта персональных данных, устанавливающие случаи обработки персональных данных несовершеннолетних, если иное не предусмотрено законодательством Российской Федерации, а также положения, допускающие в качестве условия заключения договора бездействие субъекта персональных данных (п. 5 ст. 6 Федерального закона № 152-ФЗ от 27.06.2006 г.)

5.7. Предоставление биометрических персональных данных не может быть обязательным, за исключением случаев, предусмотренных частью 2 статьи 11 Федерального закона № 152-ФЗ от 27.06.2006 г. Учреждение не вправе отказывать в обслуживании в случае отказа субъекта персональных данных предоставить биометрические персональные данные и (или) дать согласие на обработку персональных данных, если в соответствии с федеральным законом получение оператором согласия на обработку персональных данных не является обязательным. (ч. 3 ст. 11 Федерального закона № 152-ФЗ от 27.06.2006 г.)

## **6. Сбор, обработка и хранение персональных данных.**

6.1. Обработка персональных данных работника – получение, хранение, комбинирование, передача или любое другое использование персональных данных субъекта персональных данных.

Обработка персональных данных несовершеннолетних обучающихся допускается с письменного согласия родителей (законных представителей).

6.2. Порядок получения персональных данных.

6.2.1. Все персональные данные субъекта персональных данных следует получать у него самого. Если персональные данные возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Учреждение должно сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа дать письменное согласие на их получение.

6.2.2. Учреждение не имеет права получать и обрабатывать персональные данные о политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции РФ работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

6.2.3. Учреждение не имеет право получать и обрабатывать персональные данные о членстве в общественных объединениях или профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

6.3. Обработка, передача и хранение персональных данных.

К обработке, передаче и хранению персональных данных могут иметь доступ сотрудники:

- бухгалтерии;
- директор и заместитель директора;
- методист;
- тренер-преподаватель.

6.4. При передаче персональных данных Учреждение должно соблюдать следующие требования:

- не сообщать персональные данные третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях

предупреждения угрозы жизни и здоровью, а также в случаях, установленных федеральным законом;

- не сообщать персональные данные в коммерческих целях без письменного согласия;
- предупредить лиц, получающих персональные данные, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные субъекта, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными в порядке, установленном федеральными законами;
- разрешать доступ к персональным данным только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций;
- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;
- передавать персональные данные субъектов представителям работников в порядке, установленном Трудовым Кодексом, и ограничивать эту информацию только теми персональными данными, которые необходимы для выполнения указанными представителями их функций.

6.5. Передача персональных данных от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

6.6. При передаче персональных данных работника потребителям за пределы образовательного учреждения Учреждение не должно сообщать эти данные третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью или в случаях, установленных федеральным законом.

6.7. Все меры конфиденциальности при сборе, обработке и хранении персональных данных распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

6.8. Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.

6.9. По возможности персональные данные обезличиваются.

## **7. Доступ к персональным данным.**

7.1. Внутренний доступ (доступ внутри организации).

Право доступа к персональным данным сотрудника имеют:

- бухгалтерии;
- директор и заместитель директора;
- методист;
- тренер-преподаватель.
- сам работник, носитель данных.

Другие сотрудники имеют доступ к персональным данным работника только с письменного согласия самого работника, носителя данных.

7.2. Внешний доступ.

7.2.1. Предоставление персональных данных государственным органам производится в соответствии с требованиями действующего законодательства и настоящим положением.

7.2.2. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

7.2.3. Организации, в которые сотрудник может осуществлять перечисления денежных средств (страховые компании, негосударственные пенсионные фонды,

благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным работника только в случае его письменного разрешения.

7.2.4. Персональные данные сотрудника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого сотрудника.

В случае развода бывшая супруга (супруг) имеют право обратиться в организацию с письменным запросом о размере заработной платы сотрудника без его согласия. (УК РФ).

## **8. Защита персональных данных**

Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

Защита персональных данных представляет собой жестко регламентированный и динамически технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности учреждения.

### **8.1. «Внутренняя защита».**

Регламентация доступа персонала к конфиденциальным сведениям, документам и базе данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий руководителями и специалистами учреждения. Для защиты персональных данных работников принимается ряд мер:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между работниками;
- рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание работником требований нормативно – методических документов по защите информации и сохранении тайны;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа работниками;
- воспитательная и разъяснительная работа с сотрудниками учреждения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;

#### **8.1.1. Защита персональных данных сотрудника на электронных носителях.**

Все компьютеры, содержащие персональные данные сотрудника, должны быть защищены паролем.

### **8.2. «Внешняя защита».**

Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося

совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности Учреждения, посетители, работники других организационных структур.

Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов Учреждения.

## **9. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными.**

9.1. Персональная ответственность – одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

9.2. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

9.3. Каждый сотрудник учреждения, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

9.4. Лица, виновные в нарушении установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральным законом.