Муниципальное учреждение дополнительного образования
«Спортивная школа олимпийского резерва № 19»
МУ ДО «СШОР № 19»

СОГЛАСОВАНО	УТВЕРЖДЕНО
Юрисконсульт	приказом МУ ДО «СШОР № 19»
_____ К.В. Сидорова	от 02.05.2023 г. N 01-03/71.2
«02» мая 2023 г.	

ПОЛОЖЕНИЕ
Об обработке и защите персональных данных работников учреждения, обучающихся (спортсменов) и родителей (законных представителей).

I. Общие положения.

1.1. Положение (далее – Положение) об обработке и защите персональных данных муниципального учреждения дополнительного образования «Спортивная школа олимпийского резерва № 19» (далее – учреждение) разработано в соответствии: с Конституцией Российской Федерации, Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», Федеральным законом Российской Федерации от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации», Трудовым кодексом Российской Федерации (далее – ТК РФ), другими федеральными законами и иными нормативными правовыми актами.

1.2. Положение является локальным нормативным актом муниципального учреждения дополнительного образования «Спортивная школа олимпийского резерва № 19», регламентирующим порядок обеспечения защиты персональных данных субъектов: работников учреждения, обучающихся (спортсменов) и родителей (законных представителей) обучающихся при их обработке, в том числе защиты от несанкционированного доступа, неправомерного их использования.

1.3. Настоящим Положением определяется порядок получения, обработки, хранения, передачи и любого другого использования персональных данных, права и обязанности субъектов персональных данных, а также ответственность лиц, имеющих доступ к персональным данным, за невыполнение правовых норм, регулирующих обработку и защиту персональных данных.

1.4. В настоящем Положении используются следующие основные понятия и термины:

- персональные данные - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных);

- персональные данные, разрешенные субъектом персональных данных для распространения, - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном настоящим Федеральным законом;

- оператор - государственный орган, муниципальный орган, юридическое или физическое 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;

- 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;

- автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

- распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

- предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

- блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

- 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;

- обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

- информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

- трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

1.5. Персональные данные субъектов относятся к категории конфиденциальной информации.

1.6. Все вопросы, связанные с обработкой и защитой персональных данных, не урегулированные настоящим Положением, разрешаются в соответствии с действующим законодательством Российской Федерации в области персональных данных.

II. Состав персональных данных.

2.1. Если иное не установлено Трудовым Кодексом Российской Федерации, другими федеральными законами, при заключении трудового договора лицо, поступающее на работу, предъявляет работодателю:

- паспорт или иной документ, удостоверяющий личность;
- трудовую книжку и (или) сведения о трудовой деятельности, за исключением случаев, если трудовой договор заключается впервые;
- документ, подтверждающий регистрацию в системе индивидуального (персонифицированного) учета, в том числе в форме электронного документа;
- документы воинского учета - для военнообязанных и лиц, подлежащих призыву на военную службу;

- документ об образовании и (или) о квалификации или наличии специальных знаний - при поступлении на работу, требующую специальных знаний или специальной подготовки;
- справку о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям, выданную в порядке и по форме, которые устанавливаются федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере внутренних дел, - при поступлении на работу, связанную с деятельностью, к осуществлению которой в соответствии с Трудовым Кодексом Российской Федерации, иным федеральным законом не допускаются лица, имеющие или имевшие судимость, подвергающиеся или подвергавшиеся уголовному преследованию;

2.2. В отделе кадров учреждения создаются и хранятся следующие группы документов, содержащие данные о работниках в единичном или сводном виде:

2.2.1. Документы, содержащие персональные данные работников:

- 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 (распоряжений) по кадрам;
- личные дела и трудовые книжки, (СТД-Р);
- дела, содержащие материалы аттестаций работников;
- дела, содержащие материалы внутренних расследований;
- справочно-информационный банк данных по персоналу (картотеки, журналы);
- подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству учреждения, руководителям структурных подразделений;
- четы по кадрам, направляемые в государственные органы статистики, вышестоящие органы управления и другие учреждения.

2.2.2. Документация по организации работы структурных подразделений:

- должностные инструкции работников;
- приказы, распоряжения, указания руководства учреждения по основной деятельности (подлинники или копии).

2.3. К персональным данным обучающихся (спортсменов) и их законных представителей, подлежащим обработке и хранению в порядке, предусмотренном действующим законодательством и настоящим Положением, относятся следующие сведения и документы, содержащиеся в информационной системе учреждения:

- сведения, содержащиеся в документах, удостоверяющих личность занимающегося (свидетельство о рождении или паспорт);
- сведения о составе семьи;
- паспортные данные родителей (законных представителей) обучающихся;
- документы, подтверждающие права на дополнительные гарантии и компенсации по определенным основаниям, предусмотренным законодательством и локальными актами учреждения;
- номера телефонов, обучающихся и родителей (законных представителей) обучающихся;
- адрес места регистрации и фактического места жительства обучающихся (в случае если адрес места регистрации и фактического места проживания не совпадают);

- сведения, содержащиеся в справке об отсутствии у поступающего медицинских противопоказаний для прохождения спортивной подготовки по выбранному виду спорта;
- документ, подтверждающий регистрацию в системе индивидуального (персонифицированного) учета;
- сведения, содержащиеся в полисе добровольного медицинского страхования.

III. Условия обработки персональных данных.

3.1. При определении объема и содержания, обрабатываемых персональных данных, учреждение руководствуется Конституцией РФ, ТК РФ и иными федеральными законами.

3.2. Обработка персональных данных осуществляется исключительно в целях:
- обеспечения соблюдения законов и иных нормативных правовых актов;
- содействия работникам в трудоустройстве;
- организации спортивной подготовки обучающихся;
- обеспечения личной безопасности работников и обучающихся учреждения;
- контроля количества и качества выполняемой работы;
- контроля процесса спортивной подготовки обучающихся;
- обеспечения сохранности имущества.

3.2.1. Персональные данные следует получать у самого субъекта с его письменного согласия. Если персональные данные субъекта возможно получить только у третьей стороны, то субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие.

При получении персональных данных необходимо сообщить субъекту о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа на их получение.

3.2.2. Уполномоченное лицо не имеет права получать и обрабатывать персональные данные субъектов о политических, религиозных и иных убеждениях и частной жизни.

Уполномоченное лицо не имеет права получать и обрабатывать персональные данные субъектов о членстве в общественных объединениях или профсоюзной деятельности, за исключением случаев, предусмотренных ТК РФ или иными федеральными законами.

1.2.3. При получении персональных данных не от работника (за исключением случаев, если персональные данные были предоставлены работодателю на основании федерального закона или если персональные данные являются общедоступными), работодатель до начала обработки таких персональных данных обязан предоставить работнику следующую информацию:
- наименование (фамилия, имя, отчество) и адрес оператора или его представителя;
- цель обработки персональных данных и ее правовое основание;
- предполагаемые пользователи персональных данных;
- установленные законодательством права субъекта персональных данных.

3.2.4. Обработка персональных данных субъектов возможна без их согласия в следующих случаях:
- персональные данные являются общедоступными;
- персональные данные относятся к состоянию здоровья и их обработка необходима для защиты жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта невозможно;
- по требованию полномочных государственных органов в случаях, предусмотренных федеральным законом.

Работники должны быть ознакомлены под поспись с документами работодателя, устанавливающими порядок обработки персональных данных, а также об их правах и обязанностях в этой области.

3.2. Особенности обработки персональных данных, осуществляемой без использования средств автоматизации.

3.2.1. Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы (далее - персональные данные), считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

3.2.2. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее - материальные носители), в специальных разделах или на полях форм (бланков).

3.2.3. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

3.2.4. Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе сотрудники организации-оператора или лица, осуществляющие такую обработку по договору с оператором), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется оператором без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации (при их наличии).

3.2.5. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;
- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных;
- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими

персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

3.2.6. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

- при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

- при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

3.2.7. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

3.2.8. уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

3.3. Обработка персональных данных с использованием средств автоматизации.

3.3.1. Обработка персональных данных в информационной системе персональных данных с использованием средств автоматизации осуществляется в соответствии с Приказом ФСТЭК России от 18.02.2013 N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" и требованиями Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативных и руководящих документов уполномоченных федеральных органов исполнительной власти.

3.3.2. Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы, определенные в соответствии с частью 5 статьи 19 Федерального закона "О персональных данных".

3.3.3. Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

3.4. Особенности обработки персональных данных, разрешенных субъектом персональных данных для распространения.

3.4.1. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных. Оператор обязан обеспечить субъекту персональных данных возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

3.4.2. В случае раскрытия персональных данных неопределенному кругу лиц самим субъектом персональных данных без предоставления оператору согласия, обязанность предоставить доказательства законности последующего распространения или иной обработки таких персональных данных лежит на каждом лице, осуществившем их распространение или иную обработку.

3.4.3. В случае, если персональные данные оказались раскрытыми неопределенному кругу лиц вследствие правонарушения, преступления или обстоятельств непреодолимой силы, обязанность предоставить доказательства законности последующего распространения или иной обработки таких персональных данных лежит на каждом лице, осуществившем их распространение или иную обработку.

3.4.4. В случае, если из предоставленного субъектом персональных данных согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения, не следует, что субъект персональных данных согласился с распространением персональных данных, такие персональные данные обрабатываются оператором, которому они предоставлены субъектом персональных данных, без права распространения.

3.4.5. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, может быть предоставлено оператору:

- непосредственно;
- с использованием информационной системы уполномоченного органа по защите прав субъектов персональных данных.

3.4.6. В согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения, субъект персональных данных вправе установить запреты на передачу (кроме предоставления доступа) этих персональных данных оператором неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих персональных данных неограниченным кругом лиц. Отказ оператора в установлении субъектом персональных данных запретов и условий не допускается.

3.4.7. Оператор обязан в срок не позднее трех рабочих дней с момента получения соответствующего согласия субъекта персональных данных опубликовать информацию об условиях обработки и о наличии запретов и условий на обработку неограниченным кругом лиц персональных данных, разрешенных субъектом персональных данных для распространения.

3.4.8. Установленные субъектом персональных данных запреты на передачу (кроме предоставления доступа), а также на обработку или условия обработки (кроме получения доступа) персональных данных, разрешенных субъектом персональных данных для распространения, не распространяются на случаи обработки персональных данных в государственных, общественных и иных публичных интересах, определенных законодательством Российской Федерации.

3.4.9. Передача (распространение, предоставление, доступ) персональных данных, разрешенных субъектом персональных данных для распространения, должна быть прекращена в

любое время по требованию субъекта персональных данных. Данное требование должно включать в себя фамилию, имя, отчество (при наличии), контактную информацию (номер телефона, адрес электронной почты или почтовый адрес) субъекта персональных данных, а также перечень персональных данных, обработка которых подлежит прекращению. Указанные в данном требовании персональные данные могут обрабатываться только оператором, которому оно направлено.

3.4.10. Действие согласия субъекта персональных данных на обработку персональных данных, разрешенных субъектом персональных данных для распространения, прекращается с момента поступления оператору требования.

IV. Хранение и передача персональных данных.

4. Персональные данные субъектов в учреждении хранятся на бумажных и электронных носителях в специально предназначенных для этого помещениях.

4.1. Для организации хранения персональных данных в учреждении специалисты проводят мероприятия по определению круга информационных систем и совокупности обрабатываемых персональных данных, категорированию персональных данных и предварительной классификации информационных систем.

4.2. В процессе хранения персональных данных обеспечиваются:

- требования законодательства, устанавливающие правила хранения конфиденциальных сведений;
- сохранность имеющихся данных, ограничение доступа к ним в соответствии с законодательством РФ и настоящим Положением;
- контроль за достоверностью и полнотой персональных данных, их регулярное обновление и внесение по мере необходимости соответствующих изменений.

4.3. Доступ к персональным данным разрешается только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций.

4.4. Внутренний доступ к персональным данным в учреждении осуществляется в соответствии со списком лиц, уполномоченных на получение и доступ к персональным данным, утвержденным приказом руководителя учреждения.

4.5. Иные права и обязанности работников учреждения, в трудовые обязанности которых входит обработка персональных данных, определяются также должностными инструкциями.

4.6. Юридическим и физическим лицам, оказывающим услуги учреждению на основании заключенных гражданско-правовых договоров (либо на иных основаниях), которым необходим доступ к персональным данным работников учреждения в связи с выполнением ими обязательств по указанным договорам, соответствующие данные могут предоставляться работодателем только после подписания с ними соглашения о неразглашении конфиденциальной информации.

В исключительных случаях, исходя из договорных отношений с третьими лицами, допускается наличие в договорах пунктов о неразглашении конфиденциальной информации, в том числе предусматривающих защиту персональных данных субъектов.

4.7. Работники, осуществляющие обработку персональных данных, должны быть уведомлены в письменной форме о своей обязанности не разглашать персональные данные, к которым они получили доступ.

4.8. Получателями персональных данных вне учреждения на законном основании являются:

- органы пенсионного обеспечения,
- органы социального страхования, определяемые в соответствии с федеральными законами о конкретных видах обязательного социального страхования;
- органы прокуратуры, и другие правоохранительные органы;
- налоговые органы;
- инспекция труда;
- профессиональные союзы;
- иные органы и организации в соответствии с федеральными законами.

4.9. Уполномоченные лица не могут сообщать персональные данные субъектов третьей стороне без письменного согласия самого субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в других случаях, предусмотренных федеральными законами.

4.10. Работодатель обязан передавать персональные данные работника представителям работников в порядке, установленном ТК РФ и иными федеральными законами, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

4.11. Любые лица, обладающие доступом к персональным данным, обязаны соблюдать специальный режим их использования и защиты. Лица, получившие персональные данные субъекта на законном основании, обязаны использовать их исключительно в заявленных целях, а также не разглашать информацию (исключения из данного правила определяются только федеральными законами).

4.12. Лицо, которое получает личное дело другого работника во временное пользование, не имеет права делать в нем какие-либо пометки, исправления, вносить новые записи, извлекать документы из личного дела или помещать в него новые.

V. Защита персональных данных.

5.1. Защита персональных данных субъектов представляет собой регламентированный технологический, организационный и иной процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных в учреждении и обеспечивающий надежную безопасность информации.

Защита персональных данных субъектов от неправомерного их использования или утраты обеспечивается учреждением за счет его средств в порядке, установленном федеральным законом.

5.2. Для обеспечения внутренней защиты персональных данных субъектов руководитель:

- регламентирует состав работников, функциональные обязанности которых требуют соблюдения режима конфиденциальности;
- избирательно и обоснованно распределяет документы и информацию между работниками, имеющими доступ к персональным данным;
- своевременно обеспечивает работников информацией о требованиях законодательства по защите персональных данных;
- обеспечивает организацию порядка уничтожения информации;
- проводит разъяснительную работу с работниками, имеющими доступ к персональным данным, по предупреждению утраты сведений при работе с персональными данными.

5.3. Защита сведений, хранящихся в электронных базах данных учреждения, от несанкционированного доступа, искажения и уничтожения информации, а также от иных

неправомерных действий, обеспечивается разграничением прав доступа с использованием учетной записи и системой паролей.

5.4. Для обеспечения внешней защиты персональных данных субъектов руководитель:

- обеспечивает порядок приема, учета и контроля деятельности посетителей;
- организует пропускной режим;
- обеспечивает охрану помещений.

5.5. В случае выявления недостоверных персональных данных субъектов или неправомерных действий с ними на период проверки руководитель обязан осуществить блокирование персональных данных субъекта с момента обращения его самого или его законного представителя либо получения запроса уполномоченного органа по защите прав субъектов.

При выявлении неправомерных действий с персональными данными субъектов руководитель обязан устранить допущенные нарушения в срок не более трех рабочих дней от даты такого выявления.

В случае невозможности устранения допущенных нарушений руководитель не позднее чем через три рабочих дня с даты выявления неправомерности действий с персональными данными обязан уничтожить персональные данные субъекта.

5.6. В случае отзыва субъектами согласия на обработку своих персональных данных руководитель обязан прекратить обработку персональных данных субъектов и уничтожить их в срок, не превышающий трех рабочих дней от даты поступления указанного отзыва, если иное не предусмотрено соглашением между субъектами и руководителем.

5.7. Права субъектов в целях обеспечения защиты персональных данных, хранящихся в учреждении.

5.7.1. В целях обеспечения защиты персональных данных, хранящихся в учреждении, субъекты персональных данных имеют право на бесплатное получение полной информации:

- о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
- о перечне обрабатываемых персональных данных и источниках их получения;
- о сроках обработки персональных данных, в том числе сроках их хранения;
- о юридических последствиях обработки их персональных данных.

5.7.2. Субъекты персональных данных имеют право:

- на бесплатное получение полной информации о своих персональных данных и обработке этих данных;
- на свободный бесплатный доступ к своим персональным данным, в том числе на получение копий любой записи, содержащей персональные данные субъекта, за исключением случаев, предусмотренных федеральным законом;
- на определение своих представителей для защиты своих персональных данных;
- на доступ к медицинским данным, относящимся к ним, с помощью медицинского специалиста по их выбору;
- на требование об исключении или исправлении неверных, или неполных персональных данных, а также данных, обработанных с нарушением требований ТК РФ или иного федерального закона. При отказе исключить или исправить персональные данные субъекта он имеет право заявить в письменной форме руководителю учреждения о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера субъект имеет право дополнить заявлением, выражающим его собственную точку зрения;

- электроник (доступ к персональным данным, связанных с работой МУ ДО «СШОР № 19»);

VII. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных субъектов.

7.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъектов, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном ТК РФ и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

7.2. За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера работник несет дисциплинарную и материальную ответственность в порядке, установленном ТК РФ, и иную юридическую ответственность в порядке, установленном федеральным законом.

7.3. Лица, в обязанность которых входит ведение персональных данных субъектов, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

7.4. Работники учреждения, в должностные обязанности которых входит ведение личных дел обучающихся, обязаны обеспечить целостность и конфиденциальность персональных данных обучающихся, переданных им для предоставления в учреждение.

7.5. 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 влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом РФ об административных правонарушениях.

VIII. Заключение.

8.1. Руководитель обязан ознакомить работников учреждения с настоящим Положением, а также с внесенными в него изменениями и дополнениями под роспись.

В целях информирования потенциальных субъектов персональных данных данное Положение должно быть размещено в информационных системах учреждения.

8.2. Изменения и дополнения в настоящее Положение вносятся в порядке, установленном ст. 372 ТК РФ для принятия локальных нормативных актов.

Приложение 1
к Положению об обработке и защите персональных данных
работников учреждения, обучающихся (спортсменов)
и родителей (законных представителей)

Перечень информационных систем персональных данных
в МУ ДО «СШОР № 19»

№	Наименование ИСПДн
1.	Ведение бухгалтерского учета и отчетности
2.	Кадры и делопроизводство
3.	Информация о обучающихся
4.	Итоги соревновательной деятельности
5.	Сайт учреждения

Приложение 2
к Положению об обработке и защите персональных данных
работников учреждения, обучающихся (спортсменов)
и родителей (законных представителей)

**Перечень персональных данных, обрабатываемых
в МУ ДО «СШОР № 19»,
в связи с трудовыми отношениями и касающиеся
конкретного субъекта персональных данных**

№ п/п	Персональные данные	Использование персональных данных
1.	Фамилия, имя, отчества	Персонифицированный учет, налоговый учет, тарификация, штатное расписание, ведение бухгалтерского учета, ведение трудовых книжек, составление договоров, заполнение личных карточек формы Т-2, табель учета рабочего времени, заполнение журналов ведения контроля деятельности школы, выставление в СМИ, использование в документации по ведению спортивно-массовых мероприятий различного уровня, тренировочного процесса, информация на доске объявлений учреждения, отчетная документация и мониторинг, программное обеспечение спортивной деятельности, планы работы, справочник телефонов, вывески, заявки на получение медицинских полисов, заявки для повышения курсов квалификации
2.	Дата рождения	Заполнение личных карточек формы Т-2, составление договоров, использование в документации по проведению спортивно-массовых мероприятий различного уровня, тренировочного процесса, заявки на получение медицинских полисов, персонифицированный и налоговый учет
3.	Паспортные данные	Заполнение личных карточек формы Т-2, составление договоров, использование в документации по проведению спортивно-массовых мероприятий различного уровня, тренировочного процесса, заявки на получение медицинских полисов, персонифицированный и налоговый учет
4.	Адрес места жительства	Заполнение личных карточек формы Т-2, составление договоров, использование в документации по проведению спортивно-массовых мероприятий различного уровня, заявки на получение медицинских полисов, персонифицированный и налоговый учет
5.	Семейное положение (состав семьи)	Заполнение личных карточек формы Т-2 Использование в документации по проведению спортивно-массовых мероприятий различного уровня, тренировочного процесса
	Социальное положение	Документы в налоговую службу, справка 2НДФЛ, заполнение личных карточек формы Т-2
	Номер телефона (сотовый, рабочий, домашний)	Заполнение личных карточек формы Т-2, для прямого контакта, справочник телефонов, приказы учреждения по основной деятельности и личному составу Использование в документации по проведению спортивно-массовых мероприятий различного уровня, тренировочного процесса
	Образование	Заполнение личных карточек формы Т-2, использование в документации по проведению спортивно-массовых мероприятий

		различного уровня, тренировочного процесса, составление договоров, тарификация, штатное расписание, документация для лицензирования образовательной деятельности учреждения
	Профессия	Заполнение личных карточек формы Т-2, использование в документации по проведению спортивно-массовых мероприятий различного уровня, составление договоров, тарификация, штатное расписание, документация для лицензирования образовательной деятельности учреждения
	Квалификация	Заполнение личных карточек формы Т-2, использование в документации по проведению спортивно-массовых мероприятий различного уровня, составление договоров, тарификация, штатное расписание, документация для лицензирования образовательной деятельности учреждения
	Доходы	Пенсионный фонд, налоговая служба, подача сведений учредителю, информация для департамента финансов
	Номер пенсионного свидетельства	Заполнение личных карточек формы Т-2, использование в документации по проведению спортивно-массовых мероприятий различного уровня, составление договоров, пенсионный фонд
	Номер медицинского полиса	Для прохождения медицинских осмотров
	Биометрические персональные данные (физиологические особенности человека, фотографии)	Заявка на спец. одежду. При приеме занимающегося в учреждение.

Приложение 3
к Положению об обработке и защите персональных данных
работников учреждения, обучающихся (спортсменов)
и родителей (законных представителей)

ПОРЯДОК ДОСТУПА
работников МУ ДО «СШОР № 19» в помещения, в которых ведется обработка персональных данных

1. Порядок доступа работников МУ ДО «СШОР № 19» в помещения, в которых ведется обработка персональных данных (далее - Порядок), определяет правила доступа в помещения, где хранятся и обрабатываются персональные данные, в целях исключения несанкционированного доступа к персональным данным, а также обеспечения безопасности персональных данных от уничтожения, изменения, блокирования, копирования, распространения, а также от неправомерных действий в отношении персональных данных.

2. К помещениям, в которых ведется обработка персональных данных, относятся помещения, в которых происходит обработка персональных данных, как с использованием средств автоматизации, так и без таковых, а также хранятся резервные копии персональных данных и ключевые документы к ним.

3. Доступ в помещения МУ ДО «СШОР № 19» (далее - Учреждение), в которых ведется обработка персональных данных, осуществляется в соответствии с Приказом «Об установлении списка лиц, имеющих доступ к персональным данным работников МУ ДО «СШОР № 19».

4. Для помещений, в которых ведется обработка персональных данных, организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей информации, содержащих персональные данные, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц. Данный режим должен обеспечиваться в том числе:

- запиранием помещения на ключ, в том числе при выходе из него в рабочее время;
- закрытием металлических шкафов и сейфов, где хранятся носители информации, содержащие персональные данные, во время отсутствия в помещении работников, имеющих доступ.

5. Доступ посторонних лиц в помещения, в которых ведется обработка персональных данных, возможен только ввиду служебной необходимости.

На момент присутствия посторонних лиц в помещении, в котором ведется обработка персональных данных, должны быть приняты меры по недопущению ознакомления посторонних лиц с персональными данными.

6. Ответственность за соблюдение порядка доступа в помещения, в которых ведется обработка персональных данных, возлагается на работника, уполномоченного на обработку персональных данных.

Приложение 4
к Положению об обработке и защите персональных данных
работников учреждения, обучающихся (спортсменов)
и родителей (законных представителей)

**Порядок определения уровня защищенности ПДн,
угроз безопасности ПДн, актуальных при обработке ПДн в ИСПДн
и мер по обеспечению безопасности ПДн
в МУ ДО «СШОР № 19»**

I. Угрозы безопасности ПДн, актуальные при обработке ПДн в ИСПДн МУ ДО «СШОР № 19».

1. К угрозам безопасности персональных данных, актуальным при обработке персональных данных в информационных системах персональных данных МУ ДО «СШОР № 19» (далее - информационные системы), относятся:

- угрозы безопасности персональных данных, защищаемых без использования средств криптографической защиты информации (далее - СКЗИ);
- угрозы целенаправленных действий с использованием аппаратных и (или) программных средств с целью нарушения безопасности защищаемых с использованием СКЗИ персональных данных или создания условий для этого.

2. Угрозы безопасности персональных данных, защищаемых без использования СКЗИ, включают:

1) угрозы, связанные с особенностями функционирования технических, программно-технических и программных средств, обеспечивающих хранение, обработку и передачу информации;

2) угрозы несанкционированного доступа (воздействия) к персональным данным лицами, обладающими полномочиями в информационных системах, в том числе в ходе создания, эксплуатации, технического обслуживания и (или) ремонта, модернизации, снятия с эксплуатации информационных систем;

3) угрозы воздействия вредоносного кода, вредоносной программы, внешних по отношению к информационным системам;

4) угрозы использования методов воздействия на лиц, обладающих полномочиями в информационных системах;

5) угрозы несанкционированного доступа (воздействия) к отчуждаемым носителям персональных данных, включая переносные персональные компьютеры пользователей информационных систем;

6) угрозы несанкционированного доступа (воздействия) к персональным данным лицами, не обладающими полномочиями в информационных системах, с использованием уязвимостей в организации защиты персональных данных;

7) угрозы несанкционированного доступа (воздействия) к персональным данным лицами, не обладающими полномочиями в информационных системах, с использованием уязвимостей в системном и прикладном программном обеспечении информационных систем;

8) угрозы несанкционированного доступа (воздействия) к персональным данным лицами, не обладающими полномочиями в информационных системах, с использованием уязвимостей в обеспечении защиты сетевого взаимодействия и каналов передачи данных, в том числе с использованием протоколов межсетевого взаимодействия;

9) угрозы несанкционированного доступа (воздействия) к персональным данным лицами, не обладающими полномочиями в информационных системах, с использованием уязвимостей в обеспечении защиты вычислительных сетей информационных систем;

10) угрозы несанкционированного доступа (воздействия) к персональным данным лицами, не обладающими полномочиями в информационных системах, с использованием уязвимостей, вызванных несоблюдением требований по эксплуатации средств защиты информации;

11) угрозы, связанные с возможностью использования новых информационных технологий.

3. Угрозы целенаправленных действий с использованием аппаратных и (или) программных средств с целью нарушения безопасности защищаемых с использованием СКЗИ персональных данных или создания условий для этого включают:

1) создание способов, подготовка и проведение атак без привлечения специалистов в области разработки и анализа СКЗИ;

2) создание способов, подготовка и проведение атак на различных этапах жизненного цикла СКЗИ;

3) проведение атаки нарушителем, находясь вне пространства, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств (далее - контролируемая зона);

4) проведение на этапах разработки (модернизации), производства, хранения, транспортировки СКЗИ и этапе ввода в эксплуатацию СКЗИ (пусконаладочные работы) следующих атак:

а) несение несанкционированных изменений в СКЗИ и (или) в компоненты аппаратных и программных средств, совместно с которыми штатно функционируют СКЗИ и в совокупности, представляющие среду функционирования СКЗИ (далее - СФ), которые способны повлиять на выполнение предъявляемых к СКЗИ требований, в том числе с использованием вредоносных программ;

б) внесение несанкционированных изменений в технические и организационно-распорядительные документы на СКЗИ и компоненты СФ;

5) проведение атак на этапе эксплуатации СКЗИ на:

а) персональные данные;

б) ключевую, аутентифицирующую и парольную информацию СКЗИ;

в) программные компоненты СКЗИ;

г) аппаратные компоненты СКЗИ;

д) программные компоненты СФ, включая программное обеспечение базовых систем ввода (вывода);

е) аппаратные компоненты СФ;

ж) данные, передаваемые по каналам связи;

з) иные объекты, которые установлены при формировании совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак с учетом применяемых в информационной системе информационных технологий, аппаратных средств (далее - АС) и программного обеспечения (далее - ПО);

6) получение из находящихся в свободном доступе источников (включая информационно-телекоммуникационные сети, доступ к которым не ограничен определенным кругом лиц, в том числе информационно-телекоммуникационную сеть "Интернет") следующей информации об информационной системе, в которой используется СКЗИ:

а) общие сведения об информационной системе, в которой используется СКЗИ (назначение, состав, оператор, объекты, в которых размещены ресурсы информационной системы);

б) сведения об информационных технологиях, базах данных, АС, ПО, используемых в информационной системе совместно с СКЗИ, за исключением сведений, содержащихся только в конструкторской документации на информационные технологии, базы данных, АС, ПО, используемые в информационной системе совместно с СКЗИ;

в) содержание конструкторской документации на СКЗИ;

г) содержание находящейся в свободном доступе документации на аппаратные и программные компоненты СКЗИ и СФ;

д) общие сведения о защищаемой информации, используемой в процессе эксплуатации СКЗИ;

е) сведения о каналах связи, по которым передаются защищаемые СКЗИ персональные данные (далее - канал связи);

ж) данные, передаваемые в открытом виде по каналам связи, не защищенным от несанкционированного доступа к информации организационными и техническими мерами;

з) сведения о нарушениях правил эксплуатации СКЗИ и СФ в каналах связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами;

и) сведения о неисправностях и сбоях аппаратных компонентов СКЗИ и СФ, проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами;

к) сведения, получаемые в результате анализа сигналов от аппаратных компонентов СКЗИ и СФ;

7) применение:

а) находящихся в свободном доступе или используемых за пределами контролируемой зоны АС и ПО, включая аппаратные и программные компоненты СКЗИ и СФ;

б) специально разработанных АС и ПО;

8) использование на этапе эксплуатации в качестве среды переноса от субъекта к объекту (от объекта к субъекту) атаки действий, осуществляемых при подготовке и (или) проведении атаки:

а) каналов связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами;

б) каналов распространения сигналов, сопровождающих функционирование СКЗИ и СФ;

9) проведение на этапе эксплуатации атаки из информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц, если информационные системы, в которых используются СКЗИ, имеют выход в эти сети;

10) использование на этапе эксплуатации находящихся за пределами контролируемой зоны АС и ПО из состава средств информационной системы, применяемых на местах эксплуатации СКЗИ (далее - штатные средства);

11) проведение атаки при нахождении в пределах контролируемой зоны;

12) на этапе эксплуатации СКЗИ возможное уничтожение и несанкционированный доступ к:

а) документации на СКЗИ и компоненты СФ;

б) помещениям, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее - СВТ), на которых реализованы СКЗИ и СФ;

13) получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации:

а) сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы;

б) сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы;

в) сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ;

14) использование штатных средств, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий;

15) физический доступ к СВТ, на которых реализованы СКЗИ и СФ;

16) наличие у нарушителя аппаратных компонентов СКЗИ и СФ, реализованных в информационной системе, в которой используется СКЗИ.

II. Определение уровня защищенности ПДн.

1. Под уровнем защищенности персональных данных (УЗ) понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию

определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (ИСПДн).

2. Определение уровня защищенности персональных данных ИСПДн МУ ДО «СШОР № 19» проводится в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства РФ от 01.11.2012 №1119.

3. Уровни защищенности персональных данных при их обработке в ИСПДн определяются в зависимости от типа актуальных угроз безопасности персональных данных с учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные (Таблица 1).

Таблица 1.

Уровни защищенности персональных данных в ИСПДн

Категории персональных данных	**Категория субъектов**	**Количество субъектов**	**Тип актуальных угроз**		
			1 тип	**2 тип**	**3 тип**
Специальные	не сотрудников оператора	более 100000	УЗ1	УЗ1	УЗ2
		менее 100000	УЗ1	УЗ2	УЗ3
	сотрудников оператора	любое	УЗ1	УЗ2	УЗ3
Биометрические	не сотрудников оператора	более 100000	УЗ1	УЗ2	УЗ3
		менее 100000	УЗ1	УЗ2	УЗ3
	сотрудников оператора	любое	УЗ1	УЗ2	УЗ3
Иные	не сотрудников оператора	более 100000	УЗ1	УЗ2	УЗ3
		менее 100000	УЗ1	УЗ3	УЗ4
	сотрудников оператора	любое	УЗ1	УЗ3	УЗ4
Общедоступные	не сотрудников оператора	более 100000	УЗ2	УЗ2	УЗ4
		менее 100000	УЗ2	УЗ3	УЗ4
	сотрудников оператора	любое	УЗ2	УЗ3	УЗ4

4. Для определения уровня защищенности персональных данных ИСПДн в МУ ДО «СШОР № 19» создается комиссия по определению уровня защищенности приказом руководителя учреждения.

По результатам проделанной работы комиссия составляет акт определения уровня защищенности персональных данных информационной системы персональных данных и предоставляет его для утверждения руководителю учреждения.

III. Меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

1. Меры по обеспечению безопасности персональных данных принимаются для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

2. Меры по обеспечению безопасности персональных данных реализуются в рамках системы защиты персональных данных, создаваемой в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119, и должны быть направлены на нейтрализацию актуальных угроз безопасности персональных данных.

3. В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности персональных данных;
- обеспечение целостности информационной системы и персональных данных;
- обеспечение доступности персональных данных;
- защита среды виртуализации;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;
- управление конфигурацией информационной системы и системы защиты персональных данных.

Состав и содержание мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных, приведены в Таблице 2:

Таблица 2.

Состав и содержание мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных.

обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности персональных данных			
		4	3	2	1

I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)					
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+	+	+	+
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных			+	+
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+	+	+	+
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	+	+	+	+
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+	+	+	+
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	+	+	+	+
II. Управление доступом субъектов доступа к объектам доступа (УПД)					
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	+	+	+	+
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	+	+	+	+
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами	+	+	+	+
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	+	+	+	+
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	+	+	+	+
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	+	+	+	+
УПД.7	Предупреждение пользователя при его входе в				

	информационную систему о том, что в информационной системе реализованы меры по обеспечению безопасности персональных данных, и о необходимости соблюдения установленных оператором правил обработки персональных данных				
УПД.8	Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему				
УПД.9	Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы				
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу		+	+	+
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации		+	+	+
УПД.12	Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки				
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	+	+	+	+
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	+	+	+	+
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств	+	+	+	+
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	+	+	+	+
УПД.17	Обеспечение доверенной загрузки средств вычислительной техники			+	+
III. Ограничение программной среды (ОПС)					
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения				
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение			+	+

	компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения				
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов				+
ОПС.4	Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов				
IV. Защита машинных носителей персональных данных (ЗНИ)					
ЗНИ.1	Учет машинных носителей персональных данных			+	+
ЗНИ.2	Управление доступом к машинным носителям персональных данных			+	+
ЗНИ.3	Контроль перемещения машинных носителей персональных данных за пределы контролируемой зоны				
ЗНИ.4	Исключение возможности несанкционированного ознакомления с содержанием персональных данных, хранящихся на машинных носителях, и (или) использования носителей персональных данных в иных информационных системах				
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители персональных данных				
ЗНИ.6	Контроль ввода (вывода) информации на машинные носители персональных данных				
ЗНИ.7	Контроль подключения машинных носителей персональных данных				
ЗНИ.8	Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания		+	+	+
V. Регистрация событий безопасности (РСБ)					
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	+	+	+	+
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	+	+	+	+
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени	+	+	+	+

	хранения				
РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти				
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них			+	+
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе				
РСБ.7	Защита информации о событиях безопасности	+	+	+	+
VI. Антивирусная защита (АВЗ)					
АВЗ.1	Реализация антивирусной защиты	+	+	+	+
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+	+	+	+
VII. Обнаружение вторжений (СОВ)					
СОВ.1	Обнаружение вторжений			+	+
СОВ.2	Обновление базы решающих правил			+	+
VIII. Контроль (анализ) защищенности персональных данных (АНЗ)					
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей		+	+	+
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	+	+	+	+
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации		+	+	+
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации		+	+	+
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе			+	+
IX. Обеспечение целостности информационной системы и персональных данных (ОЦЛ)					

ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации			+	+
ОЦЛ.2	Контроль целостности персональных данных, содержащихся в базах данных информационной системы				
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций				
ОЦЛ.4	Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)			+	+
ОЦЛ.5	Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и (или) контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы				
ОЦЛ.6	Ограничение прав пользователей по вводу информации в информационную систему				
ОЦЛ.7	Контроль точности, полноты и правильности данных, вводимых в информационную систему				
ОЦЛ.8	Контроль ошибочных действий пользователей по вводу и (или) передаче персональных данных и предупреждение пользователей об ошибочных действиях				
X. Обеспечение доступности персональных данных (ОДТ)					
ОДТ.1	Использование отказоустойчивых технических средств				
ОДТ.2	Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы				
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование				+
ОДТ.4	Периодическое резервное копирование персональных			+	+

	данных на резервные машинные носители персональных данных				
ОДТ.5	Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала			+	+
XI. Защита среды виртуализации (ЗСВ)					
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	+	+	+	+
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	+	+	+	+
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре		+	+	+
ЗСВ.4	Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры				
ЗСВ.5	Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией				
ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных			+	+
ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций			+	+
ЗСВ.8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры			+	+
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре		+	+	+
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей		+	+	+
XII. Защита технических средств (ЗТС)					
ЗТС.1	Защита информации, обрабатываемой техническими				

	средствами, от ее утечки по техническим каналам				
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования				
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены	+	+	+	+
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	+	+	+	+
ЗТС.5	Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов)				
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)					
ЗИС.1	Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты персональных данных, функций по обработке персональных данных и иных функций информационной системы				+
ЗИС.2	Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом				
ЗИС.3	Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи	+	+	+	+
ЗИС.4	Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации)				

ЗИС.5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств				
ЗИС.6	Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с персональными данными, при обмене ими с иными информационными системами				
ЗИС.7	Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода				
ЗИС.8	Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи				
ЗИС.9	Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации				
ЗИС.10	Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам				
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов			+	+
ЗИС.12	Исключение возможности отрицания пользователем факта отправки персональных данных другому пользователю				
ЗИС.13	Исключение возможности отрицания пользователем факта получения персональных данных от другого пользователя				
ЗИС.14	Использование устройств терминального доступа для обработки персональных данных				
ЗИС.15	Защита архивных файлов, параметров настройки			+	+

	средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных				
ЗИС.16	Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер или внутри разрешенных сетевых протоколов				
ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы			+	+
ЗИС.18	Обеспечение загрузки и исполнения программного обеспечения с машинных носителей персональных данных, доступных только для чтения, и контроль целостности данного программного обеспечения				
ЗИС.19	Изоляция процессов (выполнение программ) в выделенной области памяти				
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе		+	+	+
XIV. Выявление инцидентов и реагирование на них (ИНЦ)					
ИНЦ.1	Определение лиц, ответственных за выявление инцидентов и реагирование на них			+	+
ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов			+	+
ИНЦ.3	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами			+	+
ИНЦ.4	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий			+	+
ИНЦ.5	Принятие мер по устранению последствий инцидентов			+	+
ИНЦ.6	Планирование и принятие мер по предотвращению повторного возникновения инцидентов			+	+
XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)					
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных		+	+	+

УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных		+	+	+
УКФ.3	Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных		+	+	+
УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных		+	+	+

"+" - мера по обеспечению безопасности персональных данных включена в базовый набор мер для соответствующего уровня защищенности персональных данных.

Меры по обеспечению безопасности персональных данных, не обозначенные знаком "+", применяются при адаптации базового набора мер и уточнении адаптированного базового набора мер, а также при разработке компенсирующих мер по обеспечению безопасности персональных данных.

4. В соответствии с актом определения уровня защищенности персональных данных информационной системы персональных данных комиссия вправе предложить дополнительные (компенсирующие) меры по обеспечению безопасности персональных данных.

Приложение 5
к Положению об обработке и защите персональных данных
работников учреждения, обучающихся (спортсменов)
и родителей (законных представителей)

Муниципальное учреждение дополнительного образования
«Спортивная школа олимпийского резерва № 19»
МУ ДО «СШОР № 19»

Обязательство
о неразглашении персональных данных обучающихся

Я, _____

паспорт серии _____, номер _____выдан_____

_____,

понимаю, что получаю доступ к персональным данным обучающихся МУ ДО «СШОР № 19» и во время исполнения своих обязанностей осуществляю их обработку (в том числе сбор, запись, систематизацию, накопление, хранение, уточнение, использование и передачу).

Я понимаю, что разглашение такого рода информации может нанести прямой и (или) косвенный ущерб занимающимся МУ ДО «СШОР № 19», а также МУ ДО «СШОР № 19».

В связи с этим даю обязательство при обработке персональных данных обучающихся МУ ДО «СШОР № 19» строго соблюдать требования действующего законодательства, определяющего порядок обработки персональных данных.

Я подтверждаю, что за исключением случаев и (или) при отсутствии условий, предусмотренных действующим законодательством, не имею права разглашать сведения о обучающихся МУ ДО «СШОР № 19», относящиеся к категории их персональных данных, в частности сведения: о (об) анкетных и биографических данных; образовании; составе семьи; паспортных данных; воинском учете; наличии судимостей; адресе места жительства, домашнем телефоне; месте работы или учебы членов семьи и родственников; содержании личных дел; содержании отчетов.

Я предупрежден(а) о том, что в случае нарушения мною требований действующего законодательства, определяющих режим их обработки, в том числе в случае их незаконного разглашения или утраты, я несу ответственность в соответствии с действующим законодательством, в частности ст. 90 ТК РФ.

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

_____
(дата)

Приложение 6
к Положению об обработке и защите персональных данных
работников учреждения, обучающихся (спортсменов)
и родителей (законных представителей)

Муниципальное учреждение дополнительного образования
«Спортивная школа олимпийского резерва № 19»
МУ ДО «СШОР № 19»

Обязательство о неразглашении персональных данных

работников и обучающихся

Я, _____

паспорт серии _____, номер _____выдан_____

_____, понимаю, что получаю доступ к персональным данным работников и обучающихся МУ ДО «СШОР № 19» и во время исполнения своих обязанностей осуществляю их обработку (в том числе сбор, запись, систематизацию, накопление, хранение, уточнение, использование и передачу).

Я понимаю, что разглашение такого рода информации может нанести прямой и (или) косвенный ущерб работникам и занимающимся МУ ДО «СШОР № 19», а также МУ ДО «СШОР № 19».

В связи с этим даю обязательство при обработке персональных данных работников и обучающихся МУ ДО «СШОР № 19» строго соблюдать требования действующего законодательства, определяющего порядок обработки персональных данных, а также Положения о персональных данных работников МУ ДО «СШОР № 19».

Я подтверждаю, что за исключением случаев и (или) при отсутствии условий, предусмотренных действующим законодательством, не имею права разглашать сведения о работниках и обучающихся МУ ДО «СШОР № 19», относящиеся к категории их персональных данных, в частности сведения: о (об) анкетных и биографических данных; образовании; трудовом и общем стаже; составе семьи; паспортных данных; воинском учете; заработной плате; социальных льготах; специальности; занимаемой должности; наличии судимостей; адресе места жительства, домашнем телефоне; месте работы или учебы членов семьи и родственников; содержании трудового договора; составе декларируемых сведений о наличии материальных ценностей; содержании деклараций, подаваемых в налоговую инспекцию; содержании приказов по личному составу; содержании личных дел, трудовых книжек, сведений о трудовой деятельности работников; содержании материалов, связанных с подготовкой (профессиональным образованием и профессиональным обучением) и дополнительным профессиональным образованием работников,

прохождением ими независимой оценки квалификации, их аттестацией, служебными расследованиями; содержании отчетов, направляемых в органы статистики.

Я предупрежден(а) о том, что в случае нарушения мною требований действующего законодательства и (или) Положения о персональных данных работников МУ ДО «СШОР № 19», определяющих режим их обработки, в том числе в случае их незаконного разглашения или утраты, я несу ответственность в соответствии с действующим законодательством, в частности ст. 90 ТК РФ.

С Положением о защите персональных данных работников учреждения, обучающихся (спортсменов) и родителей (законных представителей) и гарантиях их защиты ознакомлен(а).

_____	_____	_____
(должность)	(подпись)	(Ф.И.О.)

_____
(дата)

Приложение 7
к Положению об обработке и защите персональных данных
работников учреждения, обучающихся (спортсменов)
и родителей (законных представителей)

Муниципальное учреждение дополнительного образования
«Спортивная школа олимпийского резерва № 19»
МУ ДО «СШОР № 19»

Обязательство
о неразглашении персональных данных работников

Я, _____

паспорт серии _____ номер _____выдан_____

_____, понимаю, что получаю доступ к персональным данным работников МУ ДО «СШОР № 19» и во время исполнения своих обязанностей осуществляю их обработку (в том числе сбор, запись, систематизацию, накопление, хранение, уточнение, использование и передачу).

Я понимаю, что разглашение такого рода информации может нанести прямой и (или) косвенный ущерб работникам МУ ДО «СШОР № 19», а также МУ ДО «СШОР № 19».

В связи с этим даю обязательство при обработке персональных данных работников МУ ДО «СШОР № 19» строго соблюдать требования действующего законодательства, определяющего порядок обработки персональных данных, а также Положения о персональных данных работников МУ ДО «СШОР № 19».

Я подтверждаю, что за исключением случаев и (или) при отсутствии условий, предусмотренных действующим законодательством, не имею права разглашать сведения о работниках МУ ДО «СШОР № 19», относящиеся к категории их персональных данных, в частности сведения: о (об) анкетных и биографических данных; образовании; трудовом и общем стаже; составе семьи; паспортных данных; воинском учете; заработной плате; социальных льготах; специальности; занимаемой должности; наличии судимостей; адресе места жительства, домашнем телефоне; месте работы или учебы членов семьи и родственников; содержании трудового договора; составе декларируемых сведений о наличии материальных ценностей; содержании деклараций, подаваемых в налоговую инспекцию; содержании приказов по личному составу; содержании личных дел, трудовых книжек, сведений о трудовой деятельности работников; содержании материалов, связанных с подготовкой (профессиональным образованием и профессиональным обучением) и дополнительным профессиональным образованием работников, прохождением ими независимой оценки квалификации, их аттестацией, служебными расследованиями; содержании отчетов, направляемых в органы статистики.

Я предупрежден(а) о том, что в случае нарушения мною требований действующего законодательства и (или) Положения о персональных данных работников МУ ДО «СШОР № 19», определяющих режим их обработки, в том числе в случае их незаконного разглашения или утраты, я несу ответственность в соответствии с действующим законодательством, в частности ст. 90 ТК РФ.

С Положением об обработке и защите персональных данных работников учреждения, обучающихся (спортсменов) и родителей (законных представителей) и гарантиях их защиты ознакомлен(а).

_____	_____	_____
(должность)	(подпись)	(Ф.И.О.)

_____

(дата)

Приложение 8
к Положению об обработке и защите персональных данных работников учреждения, обучающихся (спортсменов) и родителей (законных представителей)

Директору МУ ДО «СШОР № 19»
Маляренко С.В.

_____

_____,
зарегистрированного(ой) по адресу_____

_____

_____

паспорт серия _____ номер _____
выдан _____

_____

СОГЛАСИЕ
на обработку персональных данных

Я, _____
(фамилия, имя, отчество полностью)

даю свое согласие муниципальному учреждению дополнительного образования «Спортивная школа олимпийского резерва № 19» (МУ ДО «СШОР № 19»), расположенному по адресу: 150054, г. Ярославль, ул. Чкалова, д. 20а на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных, а именно на сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных в соответствии со ст. 9 Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных", в целях:

№ п/п	Персональные данные	Использование персональных данных
1.	Фамилия, имя, отчества	Персонифицированный учет, налоговый учет, тарификация, штатное расписание, ведение бухгалтерского учета, ведение трудовых книжек, составление договоров, заполнение личных карточек формы Т-2, табель учета рабочего времени, заполнение журналов ведения контроля деятельности школы, выставление в СМИ, использование в документации по ведению спортивно-массовых мероприятий различного уровня, информация на доске объявлений учреждения, отчетная документация и мониторинг, программное обеспечение спортивной деятельности, планы работы, справочник телефонов, вывески, заявки на получение медицинских полисов, заявки для повышения курсов квалификации
2.	Дата рождения	Заполнение личных карточек формы Т-2, составление договоров, использование в документации по проведению спортивно-массовых мероприятий различного уровня, заявки на получение медицинских полисов, персонифицированный и налоговый учет

3.	Паспортные данные	Заполнение личных карточек формы Т-2, составление договоров, использование в документации по проведению спортивно-массовых мероприятий различного уровня, заявки на получение медицинских полисов, персонифицированный и налоговый учет
4.	Адрес места жительства	Заполнение личных карточек формы Т-2, составление договоров, использование в документации по проведению спортивно-массовых мероприятий различного уровня, заявки на получение медицинских полисов, персонифицированный и налоговый учет
5.	Семейное положение (состав семьи)	Заполнение личных карточек формы Т-2
6.	Социальное положение	Документы в налоговую службу, справка 2НДФЛ, заполнение личных карточек формы Т-2
7.	Номер телефона (сотовый, рабочий, домашний)	Заполнение личных карточек формы Т-2, для прямого контакта, справочник телефонов, приказы учреждения по основной деятельности и личному составу
8.	Образование	Заполнение личных карточек формы Т-2, использование в документации по проведению спортивно-массовых мероприятий различного уровня, составление договоров, тарификация, штатное расписание, документация для лицензирования образовательной деятельности учреждения
9.	Профессия	Заполнение личных карточек формы Т-2, использование в документации по проведению спортивно-массовых мероприятий различного уровня, составление договоров, тарификация, штатное расписание, документация для лицензирования образовательной деятельности учреждения
10.	Квалификация	Заполнение личных карточек формы Т-2, использование в документации по проведению спортивно-массовых мероприятий различного уровня, составление договоров, тарификация, штатное расписание, документация для лицензирования образовательной деятельности учреждения
11.	Доходы	Пенсионный фонд, налоговая служба, подача сведений учредителю, информация для департамента финансов
12.	Номер пенсионного свидетельства	Заполнение личных карточек формы Т-2, использование в документации по проведению спортивно-массовых мероприятий различного уровня, составление договоров, пенсионный фонд
13.	Номер медицинского полиса	Для прохождения медицинских осмотров
14.	Биометрические персональные данные (физиологические особенности человека)	Заявка на спец. одежду

Настоящее согласие действует со дня его подписания до дня отзыва в письменной форме.

_____ _____ _____

(дата) (подпись)

(расшифровка подписи)

Приложение 9
к Положению об обработке и защите персональных данных
работников учреждения, обучающихся (спортсменов)
и родителей (законных представителей)

Директору МУ ДО «СШОР № 19»
Маляренко С.В.

_____
(фамилия, имя, отчество)
зарегистрированного по адресу:
_____
_____
(адрес регистрации указывается с почтовым индексом)
паспорт серия _____ N _____
выдан_____
_____
(дата выдачи и наименование органа, выдавшего документ)

СОГЛАСИЕ
на передачу персональных данных работника третьей стороне

Я,_____,
(фамилия, имя, отчество полностью)

даю согласие МУ ДО «СШОР № 19», расположенному по адресу: 150054, г. Ярославль, ул. Чкалова, д. 20А, на предоставление
_____
(кому)
следующих моих персональных данных для _____
_____:
(цель обработки персональных данных)

_____
_____
_____
(перечень персональных данных, на обработку которых дается согласие субъекта персональных данных)

Настоящее согласие дано мной добровольно. Настоящее согласие действительно в течение одного месяца с момента его получения.

«_____» _____ 20___ г. _____/_____

Приложение 10
к Положению об обработке и защите персональных данных
работников учреждения, обучающихся (спортсменов)
и родителей (законных представителей)

Директору МУ ДО «СШОР № 19»
Маляренко С.В.

_____
(фамилия, имя, отчество)

зарегистрированного по адресу:
_____
_____
(адрес регистрации указывается с
почтовым индексом)

паспорт серия _____ N _____
выдан_____
_____
(дата выдачи и наименование органа,
выдавшего документ)

ОТЗЫВ СОГЛАСИЯ
на обработку персональных данных

Я, _____,
(фамилия, имя, отчество полностью)

в соответствии с ч. 2 ст. 9 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", отзываю у МУ ДО «СШОР № 19» согласие на обработку моих персональных данных.

Прошу прекратить обработку моих персональных данных в течение трех рабочих дней с момента поступления настоящего отзыва.

«_____» _____ 20___ г. _____/_____/
(подпись) (расшифровка)