Рассмотрено и рекомендовано на
заседании представительного органа
от «14» июля 2017 г. № 2

УТВЕРЖДЕНО
приказом директора
от 14.07.2017 г.№310/1

Политика

муниципального автономного учреждения дополнительного образования «Детско-юношеская спортивная школа №1»

в отношении обработки персональных данных сотрудников учреждения, а также учащихся и их законных представителей (родителей)

1. Общие положения

1.1. Настоящая политика (далее – Политика) разработана 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 муниципального автономного учреждения дополнительного образования «Детско-юношеская спортивная школа №1» (далее - Учреждение), определяющим ключевые направления деятельности в области обработки и защиты персональных данных, оператором которого является Учреждение.

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

1.3. Положения Политики распространяются на отношения по обработке и защите персональных данных, полученных Учреждением как до, так и после утверждения Политики, за исключением случаев, когда по причинам правового, организованного и иного характера положения Политики 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. Положения Политики 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. Основания обработки и состав персональных данных, обрабатываемых в Учреждении

2.1. Обработка персональных данных в Учреждении осуществляется в связи с выполнением функций:

- регистрации сведений, необходимых для оказания услуг родителям (законным представителям) в воспитании и образовании детей дошкольного и школьного возраста (их персональных данных), в том числе в электронном виде;
- организации работ по оказанию услуг в области образования, поддержки инновационной деятельности Учреждения;
- организации участия учащихся и сотрудников образовательных учреждений в конкурсах, семинарах, грантах, олимпиадах.

Кроме того, обработка персональных данных в Учреждении осуществляется в ходе трудовых и иных непосредственно связанных с ними отношений, в которых Учреждение выступает в качестве работодателя, в связи с реализацией Учреждением своих прав и обязанностей как юридического лица, а также при взаимодействии с органами государственной власти и местного самоуправления.

2.2. Специальные категории персональных данных, а также биометрические персональные данные Учреждением не обрабатываются.

2.3. Персональные данные получаются и обрабатываются Учреждением на основании федеральных законов, а в необходимых случаях - при наличии письменного согласия субъекта персональных данных.

2.4. В целях исполнения возложенных функций Учреждение в установленном порядке вправе поручить обработку персональных данных третьим лицам. В договоры с лицами, которым Учреждение поручает обработку персональных данных, включаются условия, обязывающие таких лиц соблюдать предусмотренные Законом о персональных данных и Политикой правила обработки персональных данных.

2.5. Учреждение предоставляет обрабатываемые ею персональные данные государственным органам и организациям, имеющим, в соответствии с федеральным законом, право на получение соответствующих персональных данных.

2.6. В Учреждении не производится обработка персональных данных, несовместимая с целями их сбора. Если иное не предусмотрено федеральным законом, по окончании обработки персональных данных в Учреждении, в том числе при достижении целей их обработки или утраты необходимости в достижении этих целей, обрабатывавшиеся Учреждением персональные данные уничтожаются или обезличиваются.

2.7. При обработке персональных данных обеспечиваются их точность, достаточность, а при необходимости - и актуальность по отношению к целям обработки. Учреждение принимает необходимые меры по удалению или уточнению неполных или неточных персональных данных.

3. Принципы обеспечения безопасности персональных данных

3.1. Основной задачей обеспечения безопасности персональных данных при их обработке в Учреждении является предотвращение несанкционированного доступа к ним третьих лиц, предупреждение преднамеренных программно-технических и иных воздействий с целью хищения персональных данных, разрушения (уничтожения) или искажения их в процессе обработки.

3.2. Для обеспечения безопасности персональных данных Учреждение руководствуется следующими принципами:

3.2.1. Обработка персональных данных должна осуществляться на законной и справедливой основе.

3.2.2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3.2.3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

3.2.4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

3.2.5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

3.2.6. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

3.2.7. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4. Доступ к обрабатываемым персональным данным

4.1. Доступ к обрабатываемым в Учреждении персональным данным имеют лица, уполномоченные приказом Учреждения, а также лица, чьи персональные данные подлежат обработке.

4.2. В целях разграничения полномочий при обработке персональных данных полномочия по реализации каждой определенной законодательством функции Учреждения закрепляются за соответствующими структурными подразделениями Учреждения.

Доступ к персональным данным, обрабатываемым в ходе реализации полномочий, закрепленным за Учреждением, могут иметь только работники Учреждения.

4.3. Доступ работников к обрабатываемым персональным данным осуществляется в соответствии с их должностными обязанностями и требованиями локальных нормативных актов Учреждения. Допуск работников к обработке персональных данных осуществляется согласно перечню типовых полномочий (ролей пользователей), утверждаемых

приказом по Учреждению. Соответствующие полномочия (роль пользователя) вносятся в должностные обязанности работников. Допущенные к обработке персональных данных работники под подпись знакомятся с документами Учреждения, устанавливающими порядок обработки персональных данных, включая документы, устанавливающие права и обязанности конкретных работников.

4.4. Факты получения доступа к информационной системе персональных данных, а также факты обработки персональных данных регистрируются, в том числе с использованием средств обеспечения информационной безопасности. Информация о фактах обработки персональных данных хранится в Учреждении, включая информационную систему, в течение трех лет.

Порядок доступа субъекта персональных данных к его персональным данным, обрабатываемым Учреждением, осуществляется в соответствии с Законом о персональных данных и определяется локальными нормативными актами Учреждения.

5. Реализация Политики

5.1. Учреждение принимает необходимые и достаточные меры для защиты обрабатываемых персональных данных от неправомерного или случайного доступа к ним, от уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий с ними со стороны третьих лиц.

5.2. Ответственность за организацию обработки персональных данных в Учреждении несет ответственный по информационной безопасности Учреждения.

Ответственный за организацию обработки персональных данных в Учреждении, в частности, обязан:

1) осуществлять внутренний контроль за соблюдением в Учреждении требований нормативных правовых актов и локальных нормативных актов в области обработки и защиты персональных данных;

2) доводить до сведения работников положения нормативных правовых актов и локальных нормативных актов Учреждения в области обработки и защиты персональных данных;

3) организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

5.3. В Учреждении разрабатываются и утверждаются директором Учреждения следующие локальные нормативные акты:

1) правила обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства РФ в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные

данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований;

2) правила рассмотрения запросов субъектов персональных данных или их представителей;

3) правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом "О персональных данных", принятыми в соответствии с ним нормативными правовыми актами и локальными актами оператора;

4) правила работы с обезличенными данными;

5) перечень информационных систем персональных данных;

6) перечни персональных данных, обрабатываемых в Учреждении в связи с реализацией трудовых отношений, а также в связи с оказанием государственных или муниципальных услуг и осуществлением государственных или муниципальных функций;

7) перечень должностей, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных;

8) перечень должностей, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;

9) должностная инструкция ответственного за организацию обработки персональных данных в Учреждении;

10) типовое обязательство служащего Учреждения, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним муниципального контракта прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей;

11) типовая форма согласия на обработку персональных данных служащих Учреждения, иных субъектов персональных данных, а также типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные;

12) порядок доступа служащих Учреждения в помещения, в которых ведется обработка персональных данных.

Документы, определяющие политику в отношении обработки персональных данных, подлежат опубликованию на официальном сайте Учреждения в течение 10 дней после их утверждения.

5.4. Учреждение осуществляет обработку персональных данных без использования средств автоматизации, а также с использованием таких средств.

5.5. При обработке персональных данных без использования средств автоматизации Учреждение в соответствии с положениями нормативных правовых актов в области обработки и защиты персональных данных реализует комплекс организационных и технических мер, обеспечивающих:

1) обособление персональных данных от информации, не содержащей персональных данных;

2) раздельную обработку и хранение каждой категории персональных данных (фиксация на отдельных материальных носителях персональных данных, цели обработки которых заведомо несовместимы);

3) соответствие типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, установленным требованиям;

4) соблюдение установленных требований при ведении журналов (реестров, книг), содержащих персональных данных, необходимых для однократного пропуска субъекта персональных данных в помещение, занимаемое Учреждением, или в иных аналогичных целях;

5) сохранность материальных носителей персональных данных;

6) условия хранения, исключающие несанкционированный доступ к персональным данным, а также смешение персональных данных (материальных носителей), обработка которых осуществляется в различных целях;

7) надлежащее уточнение, уничтожение или обезличивание персональных данных.

5.6. В соответствии с требованиями нормативных правовых актов в области обработки и защиты персональных данных обработки персональных данных с использованием средств автоматизации в Учреждении создаются информационные системы обработки персональных данных. Все информационные системы персональных данных проходят периодическую классификацию и аттестацию в соответствии с требованиями нормативных правовых актов в области обеспечения безопасности персональных данных.

Для каждой информационной системы персональных данных формируется модель угроз безопасности персональных данных и на ее основе проводятся мероприятия по обеспечению безопасности информации в соответствии с требованиями, предъявляемыми к установленному классу.

5.7. Обработка персональных данных в Учреждении с использованием средств автоматизации ведется только в информационной системе персональных данных. В Учреждении запрещается обработка персональных данных с целями, не соответствующими целям создания информационной системы персональных данных, эксплуатация информационной системы персональных данных в составе, отличном от указанного при создании информационные системы персональных данных.

5.8. Работники проходят обучение необходимым действиям по обеспечению целостности и доступности персональных данных в нештатных ситуациях.

6. Основные мероприятия по обеспечению безопасности персональных данных

6.1. В целях обеспечения управления информационной безопасностью персональных данных в Учреждении создается система защиты персональных данных (далее – СЗПД).

Объектами защиты СЗПД являются информация, обрабатываемая Учреждением и содержащая персональные данные, а также инфраструктура, содержащая и поддерживающая указанную информацию.

6.2. Обеспечение безопасности персональных данных в Учреждении реализуется:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учетом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

6.3. С целью поддержания состояния защиты персональных данных на надлежащем уровне в Учреждении осуществляется внутренний контроль за эффективностью системы защиты персональных данных и соответствием порядка и условий обработки и защиты персональных данных установленным требованиям. Внутренний контроль включает:

1) мониторинг состояния технических и программных средств, входящих в состав СЗПД;

2) контроль соблюдения требований по обеспечению безопасности персональных данных (требований нормативных правовых актов и локальных нормативных актов Учреждения в области обработки и защиты персональных данных, требований договоров, контрактов).

6.4. В целях осуществления внутреннего контроля в Учреждении проводятся периодические проверки условий обработки персональных данных. Такие проверки осуществляются ответственным за организацию обработки персональных данных в Учреждении либо комиссией, образуемой

директором Учреждения. По результатам проверки в Учреждении издается приказ.

6.5. Лица, виновные в нарушении норм, регулирующих обработку и защиту персональных данных, несут ответственность, предусмотренную законодательством Российской Федерации.