

УТВЕРЖДЕНО:
Директор МБУ ДО
«Краснотурьинская ДМШ № 1»
_____/С. М. Шотт
Приказ № 03-02/47-0 от 03.09.2026 г.

ПОЛОЖЕНИЕ
об информационной безопасности
в муниципальном бюджетном учреждении
дополнительного образования
«Краснотурьинская детская музыкальная школа № 1»

г. Краснотурьинск
2026

1. Общие положения

1. Настоящее Положение об информационной безопасности МБУ ДО «Детская музыкальная школа № 1» (далее - Положение) разработано в соответствии со следующими нормативными правовыми актами Российской Федерации Конституцией Российской Федерации, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями, внесёнными Федеральным законом от 29.12.2025 № 569-ФЗ, вступившими в силу с 01.03.2026 и 01.09.2026), Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (с изменениями, внесёнными Федеральным законом от 29.12.2025 № 569-ФЗ), Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации», Федеральным законом от 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребёнка в Российской Федерации», Федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», приказом ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» (вступил в силу 01.03.2026, с изменениями, внесёнными приказом ФСТЭК России от 08.05.2026 № 137, действующими с 01.09.2026), приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», письмом Минпросвещения России от 10.11.2025 № ИШ-2224/04 «О направлении методических рекомендаций» (Методические рекомендации по обеспечению государственных и муниципальных образовательных организаций оптимальным и безопасным доступом к государственным, муниципальным и иным информационным системам, информационно-телекоммуникационной сети «Интернет»), распоряжением Правительства Российской Федерации от 02.12.2015 № 2471-р «О Концепции информационной безопасности детей в Российской Федерации», Уставом МБУ ДО «Детская музыкальная школа № 1».

1.2. Настоящее Положение определяет систему правовых, организационных, физических и технических мер, направленных на обеспечение информационной безопасности обучающихся, работников и иных участников образовательных отношений в МБУ ДО «Детская музыкальная школа №1» (далее - Школа), защиту информационных ресурсов, персональных данных, информационных систем, технических средств, а также ограничение доступа обучающихся к информации, причиняющей вред их здоровью и (или) развитию.

1.3. Настоящее Положение определяет правила доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», защиты их от информации, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, и регулирует условия и порядок использования сети «Интернет» в Школе.

1.4. Положение обязательно для исполнения всеми работниками Школы, обучающимися и их родителями (законными представителями), а также иными лицами, имеющими доступ к информационным ресурсам и информационно-телекоммуникационной инфраструктуре Школы.

1.5. Положение утверждается приказом директора Школы и вступает в силу со дня его утверждения. Изменения и дополнения вносятся приказом директора Школы.

1.6. В Положении используются понятия, определённые федеральным законодательством в сфере информации, информационных технологий, защиты информации и защиты персональных данных.

1.7. Система информационной безопасности Школы должна обеспечивать:

1.7.1. конфиденциальность - защиту информации от несанкционированного раскрытия или перехвата;

1.7.2. целостность - точность и полноту информации и компьютерных программ;

1.7.3. доступность - возможность получения пользователями информации в пределах их компетенции.

2. Цели и задачи обеспечения информационной безопасности

2.1. Основными целями обеспечения информационной безопасности в Школе являются:

2.1.1. защита конституционных прав и свобод обучающихся, их родителей (законных представителей) и работников Школы при обработке персональных данных;

2.1.2. обеспечение защиты информации, содержащейся в информационных системах Школы, от несанкционированного доступа, уничтожения, модификации, блокирования и иных неправомерных действий;

2.1.3. ограничение доступа обучающихся к информации, причиняющей вред их здоровью и (или) развитию, в том числе распространяемой через сеть «Интернет»;

2.1.4. обеспечение непрерывности функционирования информационных систем Школы при возникновении нештатных ситуаций;

2.1.5. формирование у обучающихся, работников и родителей (законных представителей) навыков безопасного поведения в информационном пространстве.

2.2. Для достижения указанных целей решаются следующие задачи:

2.2.1. своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба;

2.2.2. создание механизма оперативного реагирования на угрозы и инциденты информационной безопасности;

2.2.3. разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам — обеспечение доступа только к тем ресурсам и выполнения только тех операций, которые необходимы конкретным пользователям для выполнения своих обязанностей;

2.2.4. обеспечение идентификации и аутентификации пользователей, участвующих в информационном обмене;

2.2.5. защита от несанкционированной модификации используемых программных средств, а также защита систем от внедрения несанкционированных программ, включая компьютерные вирусы;

2.2.6. защита информации от утечки по техническим каналам при её обработке, хранении и передаче по каналам связи;

2.2.7. обеспечение контентной фильтрации доступа к сети «Интернет»;

повышение уровня знаний и информированности работников и обучающихся по вопросам защиты информации.

3. Принципы построения системы обеспечения информационной безопасности

Законность - обеспечение информационной безопасности осуществляется в соответствии с законодательством Российской Федерации.

Системность - охват всех элементов информационной инфраструктуры Школы и всех этапов обработки информации.

Комплексность - согласованное применение правовых, организационных, физических и технических мер защиты.

Непрерывность защиты - обеспечение защиты на всех стадиях создания, развития, эксплуатации и вывода из эксплуатации информационных систем.

Своевременность - упреждающий характер мер защиты информации.

Преемственность и совершенствование - периодическая актуализация мер защиты с учётом изменений угроз и технологий.

Персональная ответственность - ответственность каждого работника за свои действия в рамках предоставленных полномочий по доступу к информационным ресурсам.

Минимизация полномочий - предоставление пользователям минимально необходимых прав доступа для выполнения служебных обязанностей.

Гибкость - способность системы защиты адаптироваться к изменениям информационной инфраструктуры и состава угроз.

Простота применения - обеспечение удобства и прозрачности применения средств защиты для пользователей.

Обязательность контроля - регулярная проверка состояния защиты информации.

4. Субъекты и объекты информационной безопасности

4.1. Субъектами доступа к информации при обеспечении информационной безопасности Школы являются:

4.1.1. работники Школы, имеющие доступ к информационным ресурсам в рамках исполнения служебных обязанностей;

4.1.2. обучающиеся, использующие информационные ресурсы Школы в образовательных целях;

4.1.3. родители (законные представители) обучающихся, получающие доступ к информации о образовательном процессе;

посетители и иные лица, допускаемые к использованию информационных ресурсов Школы в установленном порядке.

4.2. Объектами информационной безопасности Школы являются:

4.2.1. персональные данные обучающихся, их родителей (законных представителей) и работников Школы;

4.2.2. информация ограниченного доступа, обрабатываемая в информационных системах Школы;

4.2.3. информационно-телекоммуникационная инфраструктура Школы (компьютеры, серверы, сетевое оборудование, каналы связи);

4.2.4. программное обеспечение, базы данных, электронные и материальные носители информации;

4.2.5. официальный сайт Школы и иные информационные ресурсы в сети «Интернет».

4.3. Перечисленным субъектам доступа к информации необходимо обеспечить:

4.3.1. соблюдение требований законодательства в сфере защиты информации и персональных данных;

4.3.2. конфиденциальность, целостность и доступность информации в пределах их компетенции;

4.3.3. недопущение несанкционированного доступа, использования, модификации или уничтожения информации.

5. Основные угрозы информационной безопасности

5.1. Существуют два вида угроз информационной безопасности: умышленные и непреднамеренные.

5.2. К умышленным угрозам относятся:

5.2.1. несанкционированный доступ к информационным ресурсам посторонних лиц;

5.2.2. внедрение вредоносного программного обеспечения (вирусов, троянских программ, программ-шпионов);

5.2.3. хищение, модификация или уничтожение информации;

5.2.4. компьютерные атаки, направленные на нарушение функционирования информационных систем;

5.2.5. утечка персональных данных по техническим каналам;

5.2.6. доступ обучающихся к информации, причиняющей вред их здоровью и (или) развитию, через сеть «Интернет».

5.3. К непреднамеренным угрозам относятся:

5.3.1. ошибки пользователей при вводе и обработке данных;

5.3.2. неосторожная порча или утрата носителей информации;

5.3.3. повреждение каналов связи и оборудования;

5.3.4. сбои в работе программного и аппаратного обеспечения;

5.3.5. действия, совершаемые по незнанию, невнимательности или неосторожности, без злого умысла.

5.4. К естественным угрозам относятся:

5.4.1. сбои электропитания;

5.4.2. пожары, затопления и иные стихийные бедствия;

5.4.3. неисправности оборудования, обусловленные естественным старением.

5.5. Модель возможных нарушителей определяется руководителем Школы. Типы нарушителей включают внешних нарушителей (лица, не имеющие санкционированного доступа к ресурсам Школы) и внутренних нарушителей (работники или обучающиеся, имеющие легитимный доступ и превысившие полномочия).

6. Меры, методы и средства обеспечения информационной безопасности

6.1. Правовые (законодательные) меры обеспечения информационной безопасности включают:

6.1.1. соблюдение действующих в Российской Федерации законодательных и иных нормативных правовых актов, регламентирующих правила обращения с информацией;

6.1.2. издание локальных нормативных актов Школы, определяющих мероприятия по защите информации;

6.1.3. ознакомление работников с положениями законодательства в сфере информационной безопасности и персональных данных;

6.1.4. установление ответственности за нарушения правил обработки и защиты информации.

6.2. Организационные (административные) меры включают:

6.2.1. регламентацию доступа в здание Школы;

6.2.2. регламентацию допуска работников к использованию информационных ресурсов;

6.2.3. назначение приказом директора Школы работника, ответственного за обеспечение информационной безопасности и организацию обработки персональных данных;

6.2.4. осуществление внутреннего контроля за соблюдением требований информационной безопасности;

6.2.5. обучение и инструктаж работников по вопросам информационной безопасности и защиты персональных данных не реже одного раза в три года и после компьютерных инцидентов;

6.2.6. учёт, хранение и уничтожение материальных и электронных носителей информации;

определение перечня защищаемых информационных ресурсов, информационных систем и баз данных;

6.2.7. рассмотрение в срок, не превышающий десяти рабочих дней, обращений, жалоб или претензий о нарушениях законодательства в сфере информационной безопасности и направление мотивированного ответа.

6.3. Физические меры обеспечения информационной безопасности основаны на применении механических, электронных или электронно-механических устройств для создания физических препятствий на путях несанкционированного доступа:

6.3.1. ограничение физического доступа к серверам, компьютерам и сетевому оборудованию;

6.3.2. хранение носителей информации в запираемых помещениях;

6.3.3. обеспечение контроля физической целостности средств вычислительной техники.

6.4. Технические и программно-технические меры обеспечения информационной безопасности включают:

6.4.1. идентификацию и аутентификацию пользователей (использование парольной защиты, учётных записей);

6.4.2. разграничение прав доступа пользователей к информационным ресурсам;

6.4.3. регистрацию событий безопасности (ведение журналов аудита);

6.4.4. антивирусную защиту всех рабочих станций и серверов;

6.4.5. контентную фильтрацию доступа к сети «Интернет»;

6.4.6. резервное копирование информации;

6.4.7. применение сертифицированных ФСТЭК России и (или) ФСБ России средств защиты информации;

6.4.8. блокировку самостоятельной установки обучающимися программного обеспечения;

6.4.9. использование аутентификации при доступе к Интернет-ресурсам по беспроводным каналам связи;

6.4.10. блокировку несанкционированного подключения к информационным системам Школы.

6.5. Воспитательные меры включают включение в рабочие программы воспитания и календарные планы воспитательной работы мероприятий, направленных на:

6.5.1. повышение грамотности детей по вопросам информационной безопасности;

6.5.2. развитие творческих способностей детей;

6.5.3. воспитание у детей толерантности;

6.5.4. поддержку проектов, направленных на продвижение традиционных ценностей в информационной среде;

6.5.5. повышение родительских компетенций в сфере безопасного поведения детей в информационном пространстве.

7. Организация доступа к Интернет-ресурсам и контентная фильтрация

7.1. Доступ к информации, распространяемой посредством сети «Интернет», для обучающихся предоставляется в компьютерных классах (при наличии) с применением технических и программно-аппаратных средств защиты детей от информации, причиняющей вред их здоровью и (или) развитию.

7.2. При использовании ресурсов сети «Интернет» обучающимся предоставляется доступ только к тем ресурсам, содержание которых не противоречит законодательству Российской Федерации и имеет отношение к образовательному процессу.

7.3. Школа обеспечивает применение технических, программных и организационных мер, направленных на ограничение доступа обучающихся к информации, причиняющей вред их здоровью и развитию.

7.4. Виды информации, запрещённой для распространения среди детей:

7.4.1. побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству;

7.4.2. способная вызвать желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, никотин содержащую продукцию, алкогольную и спиртосодержащую продукцию, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;

7.4.3. обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным;

7.4.4. оскорбляющая человеческое достоинство и общественную нравственность;

7.4.5. отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;

7.4.6. пропагандирующая нетрадиционные сексуальные отношения и (или) предпочтения, педофилию;

7.4.7. способная вызвать у детей желание сменить пол;

7.4.8. информация, содержащая предложения о розничной продаже дистанционным способом табачной продукции, никотин содержащей продукции и кальянов.

7.5. Для системы (сервиса) контентной фильтрации обеспечивается наличие следующих функций и возможностей:

7.5.1. контентная фильтрация входящего и исходящего трафика сети «Интернет» по протоколам HTTP/HTTPS;

7.5.2. блокировка злонамеренных ресурсов сети «Интернет»;

7.5.3. поддержка «чёрных списков» и «белых списков» ресурсов сети «Интернет»;

7.5.4. блокировка вредоносного программного обеспечения и нежелательной рекламы;

7.5.5. обеспечение антивирусной защиты пользователей при взаимодействии с ресурсами сети «Интернет» (веб-антивирус), включая анализ содержимого веб-ресурсов и получаемых/передаваемых вложений;

7.5.6. принудительное включение безопасного поиска для поисковых систем в целях блокировки нежелательной информации;

7.5.7. осуществление журналирования поисковых запросов пользователей на срок до 6 месяцев;

7.5.8. блокировка приложений популярных социальных сетей с возможностью открытия к ним доступа по запросам Школы;

7.5.9. возможность добавления ресурсов сети «Интернет» в «белый список» и «чёрный список» по запросам уполномоченных органов государственной власти и Школы.

7.6. Контроль использования обучающимися ресурсов сети «Интернет» осуществляют работники Школы. При использовании обучающимися сети «Интернет» присутствие ответственного работника обязательно.

7.7. Обучающимся в Школе запрещается:

7.7.1. самостоятельно устанавливать и удалять программное обеспечение;

7.7.2. изменять настройки операционной системы и программного обеспечения;

7.7.3. осуществлять загрузку и передачу файлов, не относящихся к образовательному процессу;

7.7.4. регистрироваться на Интернет-ресурсах без разрешения педагогического работника;

7.7.5. осуществлять доступ к ресурсам, содержание которых не соответствует задачам образования и воспитания.

7.8. Работник Школы, ответственный за обеспечение информационной безопасности (далее - Ответственный), обязан:

7.8.1. контролировать соответствие содержания и оформления печатных, аудиовизуальных и иных материалов, используемых в образовательном процессе, требованиям законодательства;

7.8.2. контролировать работу системы контентной фильтрации на территории Школы;

7.8.3. принимать информацию от работников о работе системы контентной фильтрации или реализации иных мероприятий по защите обучающихся;

7.8.4. регулировать выявленные проблемы доступными способами, при невозможности докладывать директору Школы в течение 3 рабочих дней;

7.8.5. составлять проект плана мероприятий по защите обучающихся от информации, причиняющей вред их здоровью и развитию, и контролировать его реализацию.

7.9. Проверка работоспособности системы контентной фильтрации проводится не реже одного раза в учебную четверть с оформлением акта проверки. Результаты проверки фиксируются в журнале контроля контентной фильтрации.

7.10. При получении информации об Интернет-ресурсе, содержание которого не соответствует задачам образования и воспитания либо может нарушать законодательство Российской Федерации, Ответственный обязан:

7.10.1. зафиксировать факт обнаружения ресурса в журнале регистрации случаев обнаружения запрещённых сайтов;

7.10.2. обеспечить блокировку доступа к ресурсу;

7.10.3. направить информацию о ресурсе оператору связи и (или) в уполномоченные органы.

8. Обработка и защита персональных данных

8.1. Школа осуществляет обработку персональных данных обучающихся, их родителей (законных представителей) и работников в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

8.2. Обработка персональных данных несовершеннолетних обучающихся осуществляется с согласия одного из родителей (законного представителя). Согласие оформляется при зачислении обучающегося в Школу.

8.3. Школа не обрабатывает биометрические персональные данные несовершеннолетних, за исключением случаев, прямо предусмотренных законодательством.

8.4. Работники, имеющие доступ к персональным данным, обязаны:

8.4.1. не сообщать персональные данные третьей стороне без письменного согласия субъекта персональных данных (родителя, законного представителя), кроме случаев, когда это требуется федеральными законами;

8.4.2. использовать персональные данные, полученные только от субъекта или с письменного согласия родителя (законного представителя);

8.4.3. обеспечить защиту персональных данных от неправомерного использования или утраты;

8.4.4. соблюдать требование конфиденциальности персональных данных;

8.4.5. исключать или исправлять по письменному требованию родителя (законного представителя) недостоверные или неполные персональные данные;

8.4.6. обеспечить свободный доступ родителя (законного представителя) к персональным данным обучающегося, включая право на получение копий;

8.4.7. предоставлять по требованию родителя (законного представителя) полную информацию о персональных данных обучающегося и их обработке в Школе.

8.5. Размещение фотографий, видеоизображений и иных персональных данных обучающихся на официальном сайте Школы, в социальных сетях и иных информационных ресурсах осуществляется только с письменного согласия родителей (законных представителей).

8.6. Уничтожение персональных данных осуществляется в порядке, установленном отдельным локальным актом Школы, по достижении целей обработки или при отзыве согласия субъектом персональных данных.

8.7. Школа назначает приказом директора работника, ответственного за организацию обработки персональных данных, и обеспечивает внутренний контроль соответствия обработки персональных данных требованиям законодательства.

9. Оценка состояния защиты информации и контроль

9.1. Оценка состояния защиты информации проводится на основе определения:

9.1.1. показателя, характеризующего текущее состояние защиты информации от базового уровня угроз безопасности информации (показатель защищённости) - расчёт и оценка проводятся не реже одного раза в шесть месяцев;

9.1.2. показателя, характеризующего уровень развития деятельности по защите информации (показатель уровня зрелости) - расчёт и оценка проводятся не реже одного раза в два года.

9.2. Для определения значений показателей защищённости и уровня зрелости применяются методические документы, утверждённые ФСТЭК России.

9.3. Результаты оценки доводятся до руководителя Школы в течение трёх календарных дней после завершения оценки. По решению руководителя Школы разрабатывается план мероприятий по улучшению защиты информации.

9.4. Внутренний контроль за соблюдением требований информационной безопасности осуществляется Ответственным в форме плановых и внеплановых проверок. Результаты проверок оформляются актами.

9.5. Школа обеспечивает выявление и оценку угроз безопасности информации с использованием банка данных угроз безопасности информации ФСТЭК России. При выявлении уязвимостей, сведения о которых отсутствуют в банке данных, информация о них направляется в ФСТЭК России в срок не более 5 рабочих дней.

10. Реагирование на инциденты информационной безопасности

10.1. Школа обеспечивает мониторинг информационной безопасности - сбор данных о событиях безопасности, их обработку и анализ, выявление признаков реализации угроз безопасности и нарушений требований внутренних стандартов и регламентов по защите информации.

10.2. При выявлении инцидента информационной безопасности Ответственный обязан:

10.2.1. незамедлительно принять меры по локализации инцидента и предотвращению его распространения;

10.2.2. зафиксировать факт инцидента в журнале регистрации инцидентов информационной безопасности;

10.2.3. доложить директору Школы в течение 24 часов с момента обнаружения;

10.2.4. совместно с директором определить масштаб инцидента и принять меры по устранению последствий;

10.2.5. при необходимости - взаимодействовать с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) и Центром мониторинга и управления сетью связи общего пользования.

10.3. Регламент действий на случай утечки персональных данных утверждается отдельным локальным актом Школы.

11. Обеспечение непрерывности функционирования информационных систем

11.1. Школа обеспечивает меры по непрерывности функционирования информационных систем при возникновении нештатных ситуаций, включая:

11.1.1. резервное копирование информации с периодичностью, установленной внутренним регламентом;

11.1.2. периодические проверки возможности восстановления данных из резервных копий - не реже одного раза в два года;

11.1.3. обеспечение возможности восстановления доступа авторизованных пользователей к информации, заблокированной или уничтоженной вследствие реализации угроз.

11.2. Сроки восстановления выполнения значимых функций информационных систем устанавливаются внутренним регламентом Школы в зависимости от значимости функций.

12. Повышение уровня знаний и информированности

12.1. Школа обеспечивает повышение уровня знаний и информированности работников по вопросам защиты информации. Оценка уровня знаний проводится не реже одного раза в три года или после компьютерного инцидента, произошедшего у Школы.

12.2. Все работники Школы, имеющие доступ к информационным ресурсам, проходят инструктаж по вопросам информационной безопасности и защиты персональных данных при приёме на работу и периодически в процессе работы.

12.3. Школа размещает на официальном сайте ссылки на порталы и сайты просветительской направленности по вопросам информационной безопасности, а также сведения о применяемых мерах защиты.

13. Ответственность за нарушение требований информационной безопасности

13.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту информации, в том числе персональных данных, несут дисциплинарную, гражданско-правовую, административную и уголовную ответственность в соответствии с федеральным законодательством.

13.2. Ответственность за неприменение мер защиты детей от информации, причиняющей вред их здоровью и (или) развитию, в местах, доступных для детей,

установлена статьёй 6.17 Кодекса Российской Федерации об административных правонарушениях.

13.3. Директор Школы несёт персональную ответственность за организацию и обеспечение информационной безопасности в Школе.

13.4. Ответственный за обеспечение информационной безопасности несёт ответственность за выполнение возложенных на него обязанностей в соответствии с должностной инструкцией.

14. Заключительные положения

14.1. Настоящее Положение вступает в силу со дня его утверждения приказом директора Школы.

14.2. Положение подлежит актуализации не реже одного раза в год, а также при существенных изменениях законодательства Российской Федерации в сфере информационной безопасности.

14.3. В случае изменения нормативных правовых актов Российской Федерации, регулирующих вопросы информационной безопасности, положения настоящего документа применяются в части, не противоречащей действующему законодательству, до внесения соответствующих изменений.

14.4. Все локальные нормативные акты Школы в сфере информационной безопасности должны соответствовать настоящему Положению.

14.5. Контроль за исполнением настоящего Положения осуществляет директор Школы.