ОБЩЕОБРАЗОВАТЕЛЬНАЯ АВТОНОМНАЯ
НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ «ШКОЛА «КОРИФЕЙ»
(ОАНО «Школа «Корифей»)

Принято
Педагогическим советом
ОАНО «Школа «Корифей»
(Протокол от 05.03.2026 № 1)

С учетом мнения Совета родителей
(законных представителей) обучающихся
(Протокол от 05.03.2026 № 1)

С учетом мнения Совета обучающихся
(Протокол от 05.03.2026 №1)

Утверждаю:
Директор ОАНО «Школа «Корифей»

_____ Н.Н. Копылова
Приказ № 4-О от «05» марта 2026г.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат:
020702570079B3209242193746FAF79AF4
Владелец: Копылова Наталья Николаевна
Действителен: с 17.10.2025 до 17.01.2027

ПОЛОЖЕНИЕ
ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Екатеринбург, 2026

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение об информационной безопасности (далее — Положение) определяет цели, задачи, принципы, организационные и технические меры обеспечения информационной безопасности (далее — ИБ) Общеобразовательной автономной некоммерческой организации «Школа «Корифей» (далее — Школа), а также порядок реагирования на инциденты информационной безопасности.

1.2. Положение разработано в соответствии со следующими нормативными правовыми актами:

1) Конституция Российской Федерации;
2) Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
3) Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (в действующей редакции, с учётом изменений, внесённых Федеральными законами от 14.07.2022 № 266-ФЗ, от 14.02.2024 № 11-ФЗ, от 08.08.2024 № 233-ФЗ, от 30.11.2024 № 420-ФЗ);
4) Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;
5) Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
6) Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (в части применимости);
7) Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» (в редакции Указа Президента Российской Федерации от 13.06.2024 № 500) — в части, применимой к Школе;
8) Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
9) Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
10) Приказ 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» (в редакции от 14.05.2020 № 68);
11) Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищённости»;
12) Приказ Роскомнадзора от 19.06.2025 № 140 «Об утверждении требований к обезличиванию персональных данных и методов обезличивания персональных

данных» (действует с 01.09.2025, отменил приказ Роскомнадзора от 05.09.2013 № 996);

13) Приказ Росархива от 20.12.2019 № 236;
14) Устав ОАНО «Школа «Корифей», Политика в отношении обработки персональных данных Школы, Положение об обработке и защите персональных данных Школы, Положение об электронной информационно-образовательной среде Школы.

1.3. Положение является обязательным для исполнения всеми работниками Школы, обучающимися, родителями (законными представителями) обучающихся и иными лицами, имеющими доступ к информационным ресурсам и информационным системам Школы.

1.4. Цели обеспечения информационной безопасности:

1) защита персональных данных и иной защищаемой информации от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий;
2) обеспечение конфиденциальности, целостности и доступности информационных ресурсов Школы;
3) обеспечение непрерывности образовательного процесса в условиях применения электронного обучения и дистанционных образовательных технологий;
4) минимизация рисков нарушения прав субъектов персональных данных и иных рисков информационной безопасности;
5) соблюдение требований законодательства Российской Федерации в области информационной безопасности.

1.5. Основные термины и сокращения:

1) ИБ — информационная безопасность;
2) ИС — информационная система;
3) ИСПДн — информационная система персональных данных;
4) ПДн — персональные данные;
5) ЭИОС — электронная информационно-образовательная среда;
6) СЗИ — средства защиты информации;
7) СКЗИ — средства криптографической защиты информации;
8) Реестр российского ПО — Единый реестр российских программ для электронных вычислительных машин и баз данных, формируемый в соответствии со статьёй 12.1 Федерального закона № 149-ФЗ;
9) инцидент ИБ — событие, повлёкшее или способное повлечь нарушение конфиденциальности, целостности или доступности защищаемой информации либо нарушение функционирования информационной системы.

2. ОБЪЕКТЫ ЗАЩИТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. К объектам защиты Школы относятся:

1) персональные данные работников, обучающихся, их родителей (законных представителей) и иных субъектов персональных данных, обрабатываемые Школой в соответствии с Федеральным законом № 152-ФЗ;
2) электронная информационно-образовательная среда (ЭИОС, LMS) Школы и её компоненты;

3) официальный сайт Школы, личные кабинеты пользователей, системы веб-конференций, электронные журналы и дневники;
4) базы данных кадрового, финансового, бухгалтерского, учебного учёта;
5) учётные записи пользователей информационных систем Школы и аутентификационные данные (пароли, ключевые носители, токены);
6) электронные документы и архивы Школы, в том числе документы, подписанные электронной подписью;
7) видео- и аудиозаписи учебных занятий, мероприятий с участием обучающихся;
8) сведения, составляющие охраняемую законом тайну (служебная, коммерческая, иная), за исключением сведений, отнесённых к открытым;
9) программное обеспечение, серверное и сетевое оборудование, средства защиты информации, каналы связи Школы.

2.2. Защите подлежат материальные носители информации (бумажные документы, машинные носители — жёсткие диски, USB-носители, оптические диски, мобильные устройства), используемые при обработке защищаемой информации.

3. КЛАССИФИКАЦИЯ ИНФОРМАЦИИ И РЕЖИМЫ ДОСТУПА

3.1. Информация, обрабатываемая в Школе, подразделяется на следующие категории:

1) общедоступная (открытая) информация — информация, размещаемая на официальном сайте Школы в соответствии со статьёй 29 Федерального закона № 273-ФЗ и приказом Рособрнадзора от 04.08.2023 № 1493 (в редакции от 03.07.2025 № 1353, действующей с 01.03.2026);
2) информация ограниченного доступа: персональные данные субъектов; сведения служебного характера (приказы по кадровой и основной деятельности, переписка); сведения о финансово-хозяйственной деятельности; сведения о состоянии здоровья участников образовательных отношений; иные сведения, отнесённые законодательством к информации ограниченного доступа.

3.2. По уровню защищённости информационные системы персональных данных Школы относятся к одному из четырёх уровней защищённости (УЗ-1, УЗ-2, УЗ-3, УЗ-4) в порядке, установленном постановлением Правительства Российской Федерации от 01.11.2012 № 1119, с учётом категории обрабатываемых ПДн, объёма обрабатываемых ПДн и типа актуальных угроз.

3.3. Уровень защищённости каждой ИСПДн Школы определяется актом классификации ИСПДн, утверждаемым приказом директора Школы.

3.4. По итогам определения уровня защищённости разрабатывается частная модель угроз и нарушителя, а также модель применимых мер защиты в соответствии с приложением к Приказу ФСТЭК России от 18.02.2013 № 21 и Приказом ФСБ России от 10.07.2014 № 378.

4. ОТВЕТСТВЕННЫЕ ЛИЦА ЗА ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. Общее руководство деятельностью по обеспечению информационной безопасности и персональную ответственность за состояние ИБ Школы несёт директор Школы.

4.2. В целях обеспечения ИБ приказом директора Школы назначаются:

1) ответственный за организацию обработки персональных данных (статья 22.1 Федерального закона № 152-ФЗ);
2) ответственный за обеспечение безопасности персональных данных (администратор безопасности) при их обработке в ИСПДн;
3) администратор информационных систем (системный администратор);
4) ответственный за ведение официального сайта Школы;
5) комиссия по реагированию на инциденты информационной безопасности (постоянная или формируемая по факту инцидента).

4.3. Допускается совмещение функций ответственных лиц, если это не создаёт конфликта интересов и согласуется с принципом разделения обязанностей.

4.4. Полномочия и обязанности ответственных лиц определяются настоящим Положением, Положением об обработке и защите персональных данных Школы, должностными инструкциями и приказами директора Школы.

5. ОРГАНИЗАЦИОННЫЕ МЕРЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

5.1. К организационным мерам обеспечения ИБ Школы относятся:

1) разработка и утверждение комплекта локальных нормативных актов в области ИБ и защиты ПДн;
2) определение перечней ИСПДн и ИС иного назначения; определение уровней защищённости ИСПДн;
3) разграничение прав доступа работников и обучающихся к информационным ресурсам по ролевой модели;
4) ведение журналов учёта машинных носителей информации;
5) организация режима пропуска и контроля доступа в помещения, в которых размещены технические средства ИСПДн и СЗИ;
6) инструктаж и обучение работников в области ИБ; ознакомление с локальными нормативными актами под подпись при приёме на работу;
7) контроль за соблюдением работниками требований законодательства и локальных актов в области ИБ;
8) взаимодействие с операторами связи, провайдерами, поставщиками программных и аппаратных средств, заключение договоров об обработке персональных данных по поручению (статья 6 Федерального закона № 152-ФЗ).

5.2. Школа использует программное обеспечение, включённое в Единый реестр российских программ, в случаях, предусмотренных пунктом 21 Правил, утверждённых постановлением Правительства Российской Федерации от 11.10.2023 № 1678, а также с учётом требований Указа Президента Российской Федерации от 01.05.2022 № 250 (в

редакции Указа от 13.06.2024 № 500) о приоритете отечественных средств защиты информации.

5.3. Школа ведёт учёт средств защиты информации, средств криптографической защиты информации и программного обеспечения, применяемых в ИСПДн.

6. ТЕХНИЧЕСКИЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ

6.1. Технические меры защиты информации применяются с учётом уровня защищённости ИСПДн и реализуются в соответствии с приложением к Приказу ФСТЭК России от 18.02.2013 № 21.

6.2. К базовым техническим мерам относятся:

1) идентификация и аутентификация субъектов и объектов доступа (ИАФ);
2) управление доступом субъектов к объектам доступа (УПД);
3) ограничение программной среды (ОПС);
4) защита машинных носителей информации (ЗНИ);
5) регистрация событий безопасности (логирование) (РСБ);
6) антивирусная защита (АВЗ);
7) обнаружение вторжений (СОВ);
8) контроль (анализ) защищённости информации (АНЗ);
9) обеспечение целостности информационной системы и информации (ОЦЛ);
10) обеспечение доступности информации, в том числе резервное копирование (ОДТ);
11) защита технических средств и систем связи и передачи данных (ЗТС, ЗИС);
12) управление конфигурацией информационной системы и системы защиты (УКФ);
13) защита среды виртуализации, если применима (ЗСВ).

6.3. Применяемые средства защиты информации должны быть сертифицированы (прошедшими процедуру оценки соответствия) в соответствии с требованиями ФСТЭК России и (или) ФСБ России в случаях, установленных законодательством.

6.4. С 01.01.2025 в качестве средств защиты информации в Школе используются СЗИ, страной происхождения которых не являются иностранные государства, совершающие в отношении Российской Федерации недружественные действия (требование пункта 6 Указа Президента Российской Федерации от 01.05.2022 № 250 в редакции Указа от 13.06.2024 № 500).

7. ТРЕБОВАНИЯ К ИДЕНТИФИКАЦИИ, АУТЕНТИФИКАЦИИ И ПАРОЛЬНОЙ ЗАЩИТЕ

7.1. Каждому пользователю информационных систем Школы присваивается уникальная учётная запись. Совместное использование одной учётной записи несколькими пользователями не допускается.

7.2. Пароль пользователя должен соответствовать следующим требованиям:

1) длина пароля — не менее 8 символов (для администраторов и пользователей, имеющих доступ к ПДн в значительных объёмах, — не менее 12 символов);
2) содержание заглавных и строчных букв латинского алфавита, цифр и специальных символов;

3) отсутствие в пароле общеупотребительных слов, имён, дат рождения и иных легко угадываемых последовательностей;
4) запрет на использование одного и того же пароля одновременно в нескольких системах (для административных учётных записей).

7.3. Смена пароля пользователя осуществляется не реже одного раза в 90 дней, а также во всех случаях возможной компрометации пароля (передача пароля иному лицу, утрата носителя пароля, уведомление о компрометации). Смена пароля администратора — не реже одного раза в 60 дней.

7.4. Двухфакторная (многофакторная) аутентификация является обязательной:

1) для всех учётных записей администраторов информационных систем и средств защиты информации;
2) для учётных записей педагогических работников при работе в ЭИОС, в системах электронных журналов и дневников;
3) для учётных записей лиц, имеющих доступ к ПДн в объёме, требующем УЗ-1 или УЗ-2.

7.5. Передача пароля иным лицам, его запись на доступных носителях (стикеры, незащищённые файлы), а также сохранение пароля в публичных или совместно используемых браузерах не допускаются. Каждый работник несёт персональную ответственность за сохранение конфиденциальности своих аутентификационных данных.

7.6. Учётная запись блокируется при увольнении (отчислении), длительном отсутствии или выявлении факта компрометации в сроки, установленные Положением об ЭИОС Школы.

8. ПРАВИЛА РАБОТЫ ПОЛЬЗОВАТЕЛЕЙ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ШКОЛЫ

8.1. Пользователи информационных систем Школы обязаны:

1) соблюдать требования настоящего Положения и иных локальных актов Школы в области ИБ;
2) использовать информационные системы Школы исключительно в служебных и образовательных целях;
3) обрабатывать персональные данные иных субъектов только в объёме, необходимом для выполнения должностных обязанностей, и не передавать их третьим лицам, за исключением случаев, предусмотренных законодательством или согласием субъекта;
4) незамедлительно сообщать ответственному за обеспечение безопасности ПДн о выявленных инцидентах ИБ и попытках несанкционированного доступа.

8.2. Пользователям информационных систем Школы запрещается:

5) использовать чужие учётные записи или предоставлять свои учётные записи иным лицам;
6) устанавливать и использовать на рабочих устройствах нелицензионное программное обеспечение, а также программное обеспечение, не согласованное с администратором информационных систем;
7) подключать к рабочим устройствам неучтённые машинные носители информации;

8) осуществлять несанкционированное копирование, передачу, опубликование защищаемой информации, в том числе персональных данных обучающихся, их родителей (законных представителей) и иных субъектов;
9) обходить (пытаться обходить) средства защиты информации, изменять настройки безопасности рабочих устройств без согласования с администратором информационных систем;
10) осуществлять с использованием ресурсов Школы действия, противоречащие законодательству Российской Федерации, в том числе распространять информацию, запрещённую к распространению среди несовершеннолетних в соответствии с Федеральным законом от 29.12.2010 № 436-ФЗ.

9. РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ ДАННЫХ

9.1. В Школе организуется регулярное резервное копирование информационных ресурсов в целях обеспечения доступности информации и восстановления работоспособности информационных систем после инцидентов.

9.2. Базовый регламент резервного копирования:

1) базы данных ИСПДн (электронный журнал, ЭИОС, кадровый и бухгалтерский учёт) — не реже одного раза в сутки;
2) файловые ресурсы и архивы документов — не реже одного раза в неделю;
3) резервные копии хранятся не менее одного календарного года или иного срока, установленного нормативными правовыми актами и номенклатурой дел Школы (приказ Росархива от 20.12.2019 № 236).

9.3. Резервные копии хранятся отдельно от продуктивных систем, на защищённых носителях, размещённых на территории Российской Федерации (часть 5 статьи 18 Федерального закона № 152-ФЗ в редакции, действующей с 01.07.2025).

9.4. Не реже одного раза в год проводится тестовое восстановление из резервных копий с фиксацией результатов в журнале.

10. ЗАЩИТА ОТ КОМПЬЮТЕРНЫХ АТАК И ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

10.1. В Школе реализуются следующие меры защиты от компьютерных атак и вредоносного ПО:

1) применение сертифицированных антивирусных средств с регулярным обновлением антивирусных баз;
2) использование межсетевых экранов и средств обнаружения (предотвращения) вторжений;
3) защита от распределённых атак типа «отказ в обслуживании» (DDoS) на уровне провайдера и (или) собственными средствами;
4) регулярная установка обновлений безопасности операционных систем и прикладного ПО;
5) фильтрация почтовых сообщений, в том числе защита от фишинга и нежелательной корреспонденции;

6) контроль внешних носителей и портов USB на рабочих местах, обрабатывающих ПДн;
7) периодическое сканирование информационных систем на уязвимости;
8) повышение осведомлённости работников и обучающихся в вопросах безопасности (киберграмотность).

10.2. При выявлении признаков заражения вредоносным ПО или компьютерной атаки пользователь обязан незамедлительно уведомить администратора информационных систем и ответственного за ИБ, прекратить работу с подозрительным файлом (ссылкой) и не выполнять действий, которые могут привести к распространению вредоносного ПО.

11. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ И ЛОКАЛИЗАЦИЯ БАЗ ДАННЫХ

11.1. Обработка персональных данных в Школе осуществляется в соответствии с Федеральным законом № 152-ФЗ, Положением об обработке и защите персональных данных Школы и Политикой в отношении обработки персональных данных Школы.

11.2. Сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных осуществляются на территории Российской Федерации (часть 5 статьи 18 Федерального закона № 152-ФЗ в редакции, действующей с 01.07.2025).

11.3. Передача персональных данных третьим лицам осуществляется только в случаях, предусмотренных законодательством Российской Федерации, или при наличии согласия субъекта персональных данных (его законного представителя).

11.4. Школа подаёт уведомление об обработке персональных данных в Роскомнадзор и обеспечивает актуальность сведений в Реестре операторов, осуществляющих обработку персональных данных, в соответствии со статьёй 22 Федерального закона № 152-ФЗ.

12. РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

12.1. Под инцидентом информационной безопасности понимается событие или совокупность событий, повлёкших или способных повлечь нарушение конфиденциальности, целостности или доступности защищаемой информации, а также событие, отвечающее признакам инцидента с персональными данными по части 3.1 статьи 21 Федерального закона № 152-ФЗ.

12.2. При установлении факта инцидента с персональными данными Школа в соответствии с частями 3.1 и 3.2 статьи 21 Федерального закона № 152-ФЗ:

1) в течение 24 часов с момента выявления инцидента уведомляет Роскомнадзор о произошедшем, предполагаемых причинах, предполагаемом вреде, нанесённом правам субъектов персональных данных, и о принятых мерах, а также предоставляет сведения о лице, уполномоченном на взаимодействие с Роскомнадзором;
2) в течение 72 часов с момента выявления инцидента направляет в Роскомнадзор сведения о результатах внутреннего расследования, в том числе об установленных лицах, действия которых стали причиной инцидента (при их установлении).

12.3. Уведомления направляются через Портал персональных данных Роскомнадзора (pd.rkn.gov.ru).

12.4. Порядок внутренних действий при выявлении инцидента включает:

1) фиксацию факта инцидента в журнале учёта инцидентов;
2) уведомление ответственного за обеспечение безопасности ПДн и директора Школы;
3) первоочередные меры по локализации инцидента и ограничению ущерба;
4) сбор доказательств (логи, машинные носители, переписка) с обеспечением их целостности;
5) внутреннее расследование с определением причин, объёма затронутой информации, виновных лиц;
6) меры по восстановлению функционирования информационных систем и устранению последствий;
7) меры по предупреждению аналогичных инцидентов в будущем.

13. КОНТРОЛЬ И АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

13.1. Контроль соблюдения требований ИБ в Школе осуществляется на постоянной основе администратором безопасности и ответственным за организацию обработки ПДн.

13.2. Внутренний аудит соответствия мер защиты информации требованиям законодательства проводится не реже одного раза в год. По результатам аудита составляется отчёт, утверждаемый директором Школы.

13.3. Объекты контроля и аудита:

1) наличие и актуальность локальных нормативных актов в области ИБ;
2) правильность распределения прав доступа в информационных системах;
3) фактическое применение средств защиты информации; журналы регистрации событий;
4) наличие и регулярность резервных копий, результаты тестового восстановления;
5) осведомлённость работников в области ИБ;
6) состояние машинных носителей информации, ключевых документов, СКЗИ;
7) исполнение договоров об обработке ПДн по поручению.

13.4. Результаты аудита учитываются при актуализации настоящего Положения и иных ЛНА Школы.

14. ОБУЧЕНИЕ И ПОВЫШЕНИЕ ОСВЕДОМЛЁННОСТИ РАБОТНИКОВ

14.1. Все работники Школы, имеющие доступ к информационным системам и (или) персональным данным, при приёме на работу проходят первичное ознакомление с настоящим Положением и Положением об обработке и защите персональных данных Школы под подпись.

14.2. Не реже одного раза в год для работников Школы проводится повышение осведомлённости в области ИБ (инструктажи, тренинги, в том числе по вопросам защиты от фишинга, безопасности паролей, реагирования на инциденты).

14.3. Для обучающихся Школы вопросы информационной безопасности включаются в содержание программ внеурочной деятельности и воспитательной работы (информационная гигиена, безопасное поведение в сети «Интернет», защита персональных данных).

15. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ПОЛОЖЕНИЯ

15.1. Лица, виновные в нарушении настоящего Положения, в зависимости от характера и тяжести нарушения несут дисциплинарную, гражданско-правовую, административную и уголовную ответственность в соответствии с законодательством Российской Федерации, в том числе:

1) дисциплинарную ответственность — в соответствии с Трудовым кодексом Российской Федерации (статьи 192, 193) и правилами внутреннего трудового распорядка Школы;
2) административную ответственность — по статьям 13.11, 13.11.1, 13.12, 13.13 Кодекса Российской Федерации об административных правонарушениях (с учётом изменений, внесённых Федеральным законом от 30.11.2024 № 420-ФЗ);
3) уголовную ответственность — по статьям 137, 272, 273, 274 Уголовного кодекса Российской Федерации.

15.2. Привлечение лица к ответственности не освобождает его от обязанности возместить причинённый ущерб в порядке, установленном законодательством Российской Федерации.

16. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

16.1. Настоящее Положение вступает в силу с момента его утверждения приказом директора Школы и действует до его отмены или замены новым Положением.

16.2. Изменения и дополнения в настоящее Положение вносятся при изменении законодательства Российской Федерации в области информационной безопасности и защиты персональных данных, по результатам внутреннего аудита либо по инициативе директора Школы. Изменения утверждаются приказом директора Школы.

16.3. Настоящее Положение размещается на официальном сайте Школы (за исключением сведений ограниченного доступа) и доводится до сведения работников Школы под подпись.

16.4. Вопросы, не урегулированные настоящим Положением, разрешаются в соответствии с законодательством Российской Федерации и иными локальными нормативными актами Школы.