Принято
Педагогическим советом
Протокол №1
от 29 августа 2026 года

Подписан: Анисимов Александр Васильевич
DN: C=RU, OU=директор, O="МОУ "" Коркатовский лицей"""", CN=Анисимов Александр Васильевич, E=korkat.lic@mari-el.gov.ru
Основание: Я являюсь автором этого документа
Местоположение: L

«Утверждаю»
Директор МОУ «Коркатовский лицей»
_____ А.В. Анисимов
Приказ № 53
от 29 августа 2026 года

**ПОЛОЖЕНИЕ** об информационной безопасности в МОУ «Коркатовский лицей»

## 1. Общие положения

1.1. Настоящее Положение является локальным нормативным актом МОУ «Коркатовский лицей» (далее — Организация) и регламентирует вопросы обеспечения информационной безопасности в Организации.
1.2. Положение разработано в соответствии с:

- Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;
- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- иными нормативными правовыми актами Российской Федерации в сфере информационной безопасности и защиты персональных данных.

1.3. Цель системы информационной безопасности Организации — предупреждение, своевременное выявление, локализация и ликвидация угроз информационной безопасности, обеспечение конфиденциальности, целостности и доступности информации, а также защита прав субъектов персональных данных и иных субъектов информационной деятельности.
1.4. Основные термины:

- **информационная безопасность** — состояние защищённости информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности;
- **конфиденциальность** — исключение неправомерного доступа, копирования, предоставления или распространения информации;
- **целостность** — исключение неправомерного уничтожения или изменения информации;
- **доступность** — обеспечение возможности получения информации пользователями в пределах их компетенции;
- **персональные данные** — любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных).

- 1.5. Объектами защиты являются:
- информационные ресурсы, в том числе содержащие конфиденциальную информацию и персональные данные;
- средства и системы информатизации (компьютерная техника, серверы, локальная сеть, Wi-Fi, программное обеспечение);
- носители информации (жёсткие диски, флеш-накопители, карты памяти, бумажные документы);
- каналы передачи данных (в том числе интернет-соединение).

**2. Цели и задачи**

2.1. Главная цель — реализация требований законодательства по защите информации ограниченного доступа и предотвращение ущерба от разглашения, утраты, утечки, искажения, уничтожения информации, её незаконного использования, а также от нарушения работы информационной среды Организации.
2.2. Задачи:

- защита персональных данных обучающихся, работников и иных субъектов;
- обеспечение безопасности ИТ-инфраструктуры Организации;
- организация учёта носителей конфиденциальной информации и контроля доступа к информационным ресурсам;
- внедрение организационных и технических мер по предотвращению несанкционированного доступа;
- повышение осведомлённости участников образовательного процесса по вопросам информационной безопасности.

**3. Правовые и организационные основы**

3.1. Администрация Организации определяет состав, объём и порядок защиты сведений конфиденциального характера, в том числе персональных данных, и требует от работников обеспечения их сохранности.
3.2. Приказом директора назначается ответственный за обеспечение информационной безопасности (далее — Ответственный).
3.3. Доступ к конфиденциальной информации предоставляется только работникам, которым она необходима для исполнения должностных обязанностей. Допуск осуществляется после:

- ознакомления с настоящим Положением и иными локальными актами по информационной безопасности;
- подписания обязательства о неразглашении конфиденциальной информации (включая персональные данные).
  3.4. В Организации разрабатываются и утверждаются сопутствующие документы:
- перечень защищаемых информационных ресурсов и баз данных;
- инструкция по работе со съёмными носителями информации;

- инструкция по антивирусной защите и обновлению ПО;
- правила доступа к информации для разных категорий пользователей (работники, обучающиеся, внешние пользователи);
- порядок реагирования на инциденты информационной безопасности.

3.5. Ответственный организует учёт носителей конфиденциальной информации, контроль доступа, проведение инструктажей и проверок, а также взаимодействие с внешними организациями при необходимости.

## 4. Использование сети Интернет и информационных систем

4.1. Использование сети Интернет в Организации подчинено образовательным целям и осуществляется в соответствии с законодательством и локальными актами.
4.2. Для работников:

- разрешается размещать информацию на официальных ресурсах Организации в рамках должностных обязанностей;
- запрещается размещать информацию, противоречащую законодательству, не относящуюся к деятельности Организации, нарушающую нравственные и этические нормы.

4.3. Для обучающихся:

- доступ к сети Интернет предоставляется в установленном порядке и только к ресурсам, соответствующим образовательным целям и требованиям законодательства;
- запрещается доступ к контенту, недопустимому для несовершеннолетних, осуществление сделок через интернет, загрузка файлов без разрешения, распространение оскорбительной или порочащей информации.

4.4. Технические и организационные меры:

- применение средств контентной фильтрации на компьютерах, используемых обучающимися;
- запрет самостоятельной установки программного обеспечения на рабочие станции;
- контроль доступа к Wi-Fi в местах общего пользования;
- регулярное обновление антивирусного ПО и средств защиты;
- мониторинг работоспособности системы фильтрации и оперативное реагирование на инциденты.

4.5. При обнаружении потенциально опасного ресурса пользователь обязан незамедлительно сообщить об этом Ответственному (или иному уполномоченному лицу), указав URL-адрес ресурса. Ответственный принимает меры по ограничению доступа и при необходимости информирует руководство.

## 5. Защита персональных данных

5.1. Обработка персональных данных осуществляется в соответствии с ФЗ № 152-ФЗ и локальными актами Организации.
5.2. Доступ к персональным данным предоставляется только уполномоченным работникам в объёме, необходимом для выполнения трудовых функций.
5.3. Хранение персональных данных на электронных носителях осуществляется с применением средств защиты информации (шифрование, разграничение прав доступа, резервное копирование).
5.4. Бумажные носители с персональными данными хранятся в запираемых шкафах/сейфах, доступ к ним строго ограничен.
5.5. Передача персональных данных третьим лицам допускается только в случаях и порядке, установленных законодательством.

## 6. Мероприятия по обеспечению информационной безопасности

6.1. В Организации реализуются следующие мероприятия:

- антивирусная защита и регулярное обновление ПО;
- учёт носителей конфиденциальной информации и контроль их перемещения;
- разграничение прав доступа к информационным системам и ресурсам;
- резервное копирование критически важных данных;
- проведение периодических проверок и аудитов информационной безопасности;
- обучение и инструктаж работников и обучающихся по вопросам информационной безопасности;
- реагирование на инциденты и устранение их последствий.
  6.2. План мероприятий утверждается ежегодно приказом директора и корректируется по мере необходимости.

## 7. Ответственность

7.1. Работники Организации несут дисциплинарную, материальную, административную или уголовную ответственность за нарушение требований настоящего Положения и законодательства в сфере информационной безопасности и защиты персональных данных в зависимости от характера и последствий нарушения.
7.2. Обучающиеся и иные пользователи информационных систем Организации обязаны соблюдать установленные правила и несут ответственность в порядке, предусмотренном локальными актами и законодательством.

## 8. Заключительные положения

8.1. Если нормами действующего законодательства РФ предусмотрены иные требования, чем настоящим Положением, применяются нормы законодательства РФ.
8.2. Внесение изменений и дополнений в настоящее Положение осуществляется приказом директора после согласования с Педагогическим советом и Советом обучающихся.

8.3. Настоящее Положение вступает в силу с даты его утверждения и действует до принятия новой редакции.