МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
"СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 127"
ПРИВОЛЖСКОГО РАЙОНА Г. КАЗАНИ

ПРИНЯТО:
на Педагогическом совете
Протокол № 3
от «30» 10 2025 года

УТВЕРЖДЕНО:
Директор МБОУ «Школа №127»
Ферафонтова Ф.А. _____
Приказ №287/6 от «30» 10 2025 года

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
Сертификат: 00A680A5A0CA6967A8836AC8D1C49C4173
Владелец: ФЕРАФОНТОВА ФАРИДА АЛЬФАТОВНА
Действителен с 11.03.2025 до 04.06.2026

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
Муниципального бюджетного общеобразовательного учреждения «Средняя общеобразовательная школа №127» Приволжского района г. Казани

1. Общие положения

1.1. Настоящая Политика определяет цели, задачи и принципы обеспечения информационной безопасности в МБОУ "Школа № 127" Приволжского района г. Казани, а также правила доступа к информационным ресурсам и их защиты от несанкционированного доступа (НСД) .
1.2. Политика разработана в соответствии с Конституцией РФ, Федеральным законом № 149-ФЗ «Об информации, информационных технологиях и о защите информации», № 152-ФЗ «О персональных данных», № 436-ФЗ «О защите детей от информации...», а также приказами ФСТЭК и ФСБ России .
1.3. Действие Политики распространяется на всех сотрудников школы, а также лиц, работающих по договорам гражданско-правового характера и использующих информационные ресурсы школы .

2. Цели и задачи

2.1. Основная цель – обеспечение конфиденциальности, целостности и доступности информации, обрабатываемой в информационных системах школы.
2.2. Основные задачи:
- Защита от несанкционированного доступа к информационным ресурсам .
- Разграничение доступа пользователей к ресурсам на основе должностных обязанностей (принцип минимальных привилегий) .
- Предотвращение утечки персональных данных и иной информации ограниченного распространения.
- Обеспечение правового режима использования программного обеспечения.

3. Правила доступа и работы в информационных системах

3.1. Доступ сотрудников к информационным ресурсам (электронный журнал, АИС, базы данных, файловые хранилища) разрешается только после подписания Обязательства о неразглашении персональных данных (или иного документа) и издания приказа о допуске .
3.2. Идентификация и аутентификация пользователей осуществляется с использованием уникальных логинов и паролей. Передача личных паролей другим лицам запрещена.

3.3. Запрещается установка нелицензионного программного обеспечения, а также программ, не связанных с исполнением должностных обязанностей.
3.4. При увольнении сотрудника или изменении его должностных обязанностей Ответственный за информационную безопасность обязан заблокировать или изменить его учетную запись в течение 24 часов.

4. Защита от несанкционированного доступа

4.1. В школе должны применяться сертифицированные или прошедшие оценку соответствия средства антивирусной защиты.
4.2. Должна быть организована система контент-фильтрации для ограничения доступа обучающихся к ресурсам, несовместимым с задачами образования .
4.3. Серверы и компьютеры, на которых обрабатываются персональные данные, должны быть защищены от НСД средствами разграничения доступа и находиться в контролируемой зоне (помещения, исключающие бесконтрольный доступ посторонних) .

5. Ответственность

5.1. Лица, виновные в нарушении требований настоящей Политики, разглашении персональных данных или совершении действий, приведших к НСД, несут дисциплинарную, административную или уголовную ответственность в соответствии с законодательством РФ .

Пронумеровано, прошито и

скреплено печатью на 2

двух

_____листах

директор / Р.Г. Терентьева /