MARTENSCROFT
NURSERY SCHOOL & CHILDREN'S CENTRES

Title: Information Technology (IT) Policy

School Name:	Martenscroft Nursery School
Author:	A.Davenport
Approved by:	Ajai Singh
Ratified date:	February 2026
Interim review date:	
Next Review date:	February 2027

MARTENSCROFT

NURSERY SCHOOL & CHILDREN'S CENTRES

INTRODUCTION

This policy outlines the framework for ensuring the security and integrity of the information technology systems at [School Name] Primary School. It is designed to protect the school's digital infrastructure, safeguard sensitive data, and ensure compliance with statutory obligations, including those set out by the Department for Education (DfE).

PURPOSE

- Protect the confidentiality, integrity, and availability of the school's information systems.
- Ensure the safety and security of pupils, staff, and stakeholders in the digital environment.
- Comply with relevant legislation and DfE guidance, including data protection and safeguarding requirements.

SCOPE

- All staff, pupils, governors, contractors, and third-party service providers.
- All devices, systems, and networks owned or operated by the school.
- All data processed, stored, or transmitted by the school.

ROLES AND RESPONSIBILITIES

- Headteacher: Holds overall accountability for IT security within the school.
- School Business Manager: Responsible for the implementation and monitoring of IT security measures.
- Governing Body: Provides oversight and ensures the policy is reviewed and updated annually.
- All Users: Must adhere to this policy and report any security concerns or incidents promptly.

CYBER SECURITY STANDARDS

Risk Management

- Conduct annual cyber risk assessments and review them termly.
    - Identify, assess, and mitigate risks to digital assets and services.

Awareness and Training

To ensure all staff and pupils are equipped to manage cyber risks effectively, the school will implement the following training measures:

Staff Training:

- All staff must complete the National Cyber Security Centre (NCSC) Cyber Security Training for School Staff

Training topics include:

- Recognising phishing and social engineering attacks
- Managing passwords and access securely
- Protecting devices and data
- Responding to cyber incidents

- Staff will receive a certificate of completion upon finishing the training.
- Refresher training will be provided annually or following a significant cyber incident.

Pupil Education:

- Pupils will receive age-appropriate digital safety education as part of the computing and PSHE curriculum.

Induction and Ongoing Development:

- All new staff will receive cyber security training as part of their induction.
- Ongoing updates and briefings will be provided throughout the academic year to reflect emerging threats and changes in guidance.

Technical Safeguards

- Deploy up-to-date anti-malware software and firewalls.
- Enable automatic updates on all devices.
- Encrypt sensitive data and portable devices.

Access Control

- Enforce strong password policies and, where feasible, multi-factor authentication.
- Implement role-based access controls to restrict data access.
- Deactivate unused accounts in a timely manner.

Data Backup and Recovery

- Perform daily backups of critical data to secure, off-site or cloud-based storage.
- Test data restoration procedures at least annually.

Incident Management

- Report all cyber incidents immediately to the IT Security Lead and Headteacher.
- Maintain an incident log and conduct post-incident reviews.
- Notify the Information Commissioner's Office (ICO) in the event of a data breach, where required.

FILTERING AND MONITORING

- Employ DfE-compliant web filtering and monitoring systems to:
  - Prevent access to harmful or inappropriate content.
  - Detect and respond to safeguarding concerns.
- Review filtering and monitoring policies on a termly basis.

DEVICE AND NETWORK SECURITY

- Ensure all school-owned devices meet DfE security standards.
- Maintain a secure network infrastructure with appropriate segmentation and

access controls.

- Keep an up-to-date asset register of all IT equipment.

CLOUD SERVICES AND THIRD PARTY PROVIDERS

- Use only cloud services that comply with DfE and UK GDPR requirements.
- Ensure all third-party providers sign a Data Processing Agreement (DPA) and adhere to the school's data protection standards.

POLICY REVIEW

This policy shall be reviewed annually or following any significant changes in legislation, DfE guidance, or after a major security incident.