Cyber Security

St Michael's Easthampstead CE Primary School

At St Michael's we are a community of active learners who go above and beyond in everything we do, equipping ourselves to make a difference in our own lives and in the lives of others

Policy Name	Cyber Security
Brief Description:	Sets out how our school keeps pupils, staff, systems, and data safe online.
Status: Statutory/non-statutory	Non- Statutory
Other related policies and procedures:	Behaviour Policy Safeguarding Policy Online Safety Policy Data Privacy Policies Anti-bullying Policy Bullying and Harassment Policy Home-School Agreement Codes of Conduct for: Staff, Volunteers, Parents
Approval level: HT/Governors/FGB	FGB
Approved by the Governing Board on:	23/3/2026
Frequency to be reviewed	Annually
Latest Date for Next Review:	23/3/2027
Version + Schedule of Amendments:	1
Signed:	Shaun Riordan
Position:	Headteacher
Date of Signature:	23/3/2026

Cyber Security Policy

This policy sets out how our school keeps pupils, staff, systems, and data safe online. It follows guidance from the NCSC, DfE, KCSIE, UK GDPR, and national safeguarding requirements.

---

1. Purpose and scope

Cyber security is important to protect our pupils, staff, and school systems. This policy explains how we manage online safety, keep data secure, and maintain continuity of learning.

2. Who the Policy Applies To

This policy applies to:

• All staff, governors, volunteers, and contractors

• All school IT systems, networks, devices, and cloud services

• All school and personal data processed in school

Everyone must follow the rules to keep systems and data safe.

3. Roles and Responsibilities

Accountability and responsibilities for cyber security across the school are as follows:

- **Governing Body**: Oversees cyber security, approves the policy, ensures resources, and receives regular reports.
- **Headteacher**: Responsible for overall cyber security and compliance with guidance.
- **IT Provider / IT Lead**: Makes sure systems, networks, and devices are secure; manages access, updates, backups, and incident reporting.
- **Designated Safeguarding Lead (DSL)**: Handles pupil-related online safety concerns and works with IT and DPO on incidents.
- **Data Protection Officer (DPO)**: Advises on data protection and reports breaches according to GDPR.
- **Cyber Security Liaison (SLT member):** Monitors local IT systems, reports issues, and acts as the main contact for the IT provider.
- **All Staff, Governors, and Volunteers**: Follow the rules, complete training, and report any suspected cyber incidents immediately.

4. Cyber Security Standards

The school protects systems and data through:

- **Secure accounts and passwords:** Minimum length, regular changes, 2FA where required
- **Access control:** Users only have the access they need and at appropriate levels
- **Updates and patches:** Devices are updated regularly
- **Network security:** Firewalls, internet filtering, and monitoring
- **Regular staff awareness and training**

5. Device and Network Safety

- Only school-managed devices can access school systems
- Devices are encrypted, patched, and have antivirus software
- Guest networks and school networks operate independently
- Vulnerability scans and monitoring are carried out regularly

6. Education and Training

- Staff complete regular cyber security and online safety training
- Role-specific training for users with sensitive access
- Children learn about safe online behaviour and digital risks in PSHE and ICT lessons
- Parents and carers receive regular guidance to support safe online use at home
- Third-party providers must follow the security standards outlined by our IT provider

7. Reporting Cyber Incidents

If a cyber incident happens (e.g., malware, phishing, data breach):

1. Report immediately to the IT provider, Headteacher, DPO, and DSL if pupil-related
2. Incidents are classified by severity
3. Follow the Cyber Incident Response best practice: contain the issue, communicate, preserve evidence, report to governing body and ICO if needed, review lessons learned

8. Safeguarding

- Systems protect pupils from harmful content through robust filtering and monitoring
- Concerns flagged regarding pupil or staff accounts are treated as safeguarding concerns
- Staff are trained to spot online threats and digital harm and report any such concerns to the DSL

9. Third Parties

- Suppliers are checked against school and our IT providers' security standards
- Data agreements include security requirements
- Supplier access is restricted and monitored

10. Risk Management

- Cyber security is included in the school's risk register
- Controls are reviewed annually with our IT provider
- Reports are provided to the governing body
- Compliance checks are carried out with our IT provider termly

11. Commitment to DfE Standards

The school is working towards DfE Digital and Technology Standards, including cyber security, by 2030. Current practices aim for continuous improvement in digital safety and resilience, and we continue to work with our IT provider(s) towards this.

12. Policy Review

This policy is reviewed every year, or sooner if guidance changes, a major cyber incident occurs, or technology updates require it.