Castle Camps

Cyber Security Policy

Written by: Dan Williamson

Approved on: 28/09/26

Review date: 01/10/27

Cyber Security Policy

(To be read in conjunction with the Safe Guarding and Data Protection, Acceptable Use and Critical Incidence Policies.)

---

1. Purpose

Castle Camps School recognises that cyber security is essential to safeguarding pupils, staff, data and school operations.
This policy sets out how the school meets the **Department for Education (DfE) Cyber Security Standards for Schools and Colleges** and ensures that digital systems, data and users are protected from cyber threats.

---

2. Governance, Roles and Responsibilities

2.1 Strategic Responsibility

- The **Headteacher** holds overall responsibility for cyber security within the school.
- The **Deputy Headteacher**, who also acts as **IT Co-ordinator**, is responsible for:
    - Implementing and enforcing cyber security controls
    - Managing access to systems and user accounts
    - Ensuring multi-factor authentication (MFA) is enabled
    - Liaising with the school's ICT Service and external providers

Both the Headteacher and Deputy support oversight of cyber security risks and incident response in conjunction with our Critical Incidence Policy.

2.2 Operational Responsibility

- The **ICT Service** is responsible for:
  - Configuration and management of the school firewall
  - Network filtering and monitoring
  - Ensuring only authorised devices can connect to the school network
- **All staff and governors** are responsible for:
  - Following cyber security guidance and training
  - Protecting their login credentials
  - Reporting suspected cyber incidents immediately
- **Headteacher and Deputy Headteacher** are both responsible for user management within Google and its cloud-based software, including levels of access to drives and documents. This is documented in more detail under section 4 of this policy.

---

3. Cyber Risk Assessment

- The school completes a **formal Cyber Security Assessment** to identify, assess and manage cyber risks.
- This assessment is:
  - Reviewed **at least annually**
  - Updated following any significant cyber incident or system change
- Identified risks and mitigating actions are documented and monitored by the Headteacher and Deputy Head (IT Co-ordinator).

---

4. User Accounts, Access Control and Authentication

4.1 Account Management

- All users are provided with **individual school accounts**.
- Access to systems and shared drives is granted on a **least-privilege basis**.
- Accounts are reviewed regularly and **disabled promptly** when a user leaves the school.

4.2 Multi-Factor Authentication (MFA)

- From **January 2026**, **all staff email and Google accounts** use **two-factor authentication (2FA)**.
- Staff are required to use an **authenticator app** (Microsoft Authenticator is currently the preferred choice) installed on their mobile phone.
- Authentication behaviour:
    - No MFA prompt when a device is connected to the school network (automatically detected)
    - MFA required when accessing accounts off-site or on non-school networks
- New staff are given a two-week grace period to configure MFA.
- After this period, staff who have not enabled MFA are automatically locked out of school email and Google accounts.
- Email (currently Microsoft Outlook), Google, Sonar Assessment System and MyConcern accounts require re-authentication (usually every 14 days), which is enforced automatically through the software platforms.

The Deputy Head (IT Co-ordinator) is responsible for monitoring and enforcing MFA compliance.

---

5. Network Security and Device Management

5.1 Firewall and Filtering

- All devices connected to the school network are protected by the **NetSweeper firewall**.
- Filtering and monitoring levels are applied based on user type:
    - Staff
    - Pupils
- Filtering supports safeguarding, data protection and cyber security requirements.

If Netsweeper deems any searches to be potentially malicious or inappropriate then the Headteacher is notified via email. This will state the user, date, time and the search words used.

5.2 Approved Devices Only

- **Only school-owned hardware** is permitted to connect to the school network.
- Devices from trusted external agencies may be permitted **only with the explicit approval of the Headteacher**.
- **Personal devices** belonging to staff, pupils or parents are **not permitted** to access the school network under any circumstances.

---

6. Software, Licensing and Patch Management

New software, cloud services and digital platforms must be approved by the Headteacher before use to ensure appropriate security, safeguarding, data protection and contractual requirements are met.

- All teacher laptops:
  - Run the latest supported version of Microsoft Windows
  - Are fully licensed
  - Receive automatic security updates and patches
- Automatic updates ensure continued vendor support and protection against known vulnerabilities.
- The Deputy Head (IT Co-ordinator) works with the ICT Service to ensure unsupported or unpatched devices are not used.

---

7. Data Storage, Shared Drives and Information Security

- Shared drives are managed by the **Headteacher and Deputy Head (IT Co-ordinator)**.
- By default:
  - Shared drives are **not accessible to anyone outside Castle Camps School**
  - Folder-level sharing is **disabled** to prevent accidental data exposure
- A designated **Planning Drive** exists:
  - Contains **no confidential or personal data**

    - Allows sharing so teaching resources can be uploaded to **Google Classroom**
- Any exception to these controls must be authorised by the Headteacher.

8. Data Backup and Recovery

School data is backed up in line with ICT Service procedures. The school seeks assurance from its ICT Service that backup arrangements are tested periodically and are capable of restoring critical systems and data following an incident.

- Backups are designed to:
    - Protect against data loss
    - Support recovery following a cyber incident or system failure
- Backup arrangements are reviewed as part of the annual cyber risk assessment.

---

9. Use of Artificial Intelligence (AI)

Staff may only use AI systems that have been approved by the school. Personally identifiable pupil information, safeguarding records, personnel information or other confidential school information must not be entered into AI systems unless specifically authorised by the Headteacher and covered by an appropriate data protection and risk assessment process.

Currently the pupils do not have access to any form of AI system within school but are taught relevant knowledge and skills through the school's computing curriculum.

The Headteacher and IT Co-ordinator are able to restrict access to different AI systems using the Google Admin console and through NetSweeper via the ICT Service. It is the responsibility of the Headteacher and the IT Co-ordinator to periodically review currently in use and emerging AI technologies and determine their suitability for educational or administrative use.

---

10. Cyber Awareness and Training

Cyber security training is provided to all staff and governors.

- Training includes:
  - Password security and MFA
  - Phishing and social engineering
  - Safe use of email and online platforms
  - Reporting concerns or suspected cyber incidents
- Pupils receive age-appropriate cyber security education as part of the computing curriculum. This includes safe use of digital technology and an awareness of potential malicious threats (that are age appropriate).
- Loss or theft of any school-owned device must be reported immediately to the Headteacher and Deputy Headteacher (IT Co-ordinator), regardless of whether school data is believed to be stored on the device.

---

11. Cyber Incident Reporting and Response

- Any suspected cyber incident (including phishing, malware, unauthorised access or data breach) must be reported immediately to:
  - The Deputy Head (IT Co-ordinator)
  - The Headteacher
- Incidents are:
  - Logged
  - Investigated
  - Escalated where required to external agencies (e.g. ICT Service, Local Authority, ICO)
- Lessons learned from incidents inform future risk assessments and training.

---

12. Policy Review

- This policy is reviewed:
    - Annually
    - Following any significant cyber incident
    - In line with updates to DfE cyber security standards
    - When a member of staff has left the school

DfE Cyber Security Standards – Compliance Mapping Table

DfE Cyber Security Standard	DfE Expectation	Castle Camps School Implementation	Status
1. Identify and manage cyber risks	Schools should carry out a cyber risk assessment annually and review risks regularly (at least termly).	The school is completing a **formal Cyber Security Assessment**, which identifies and mitigates cyber risks. This assessment is reviewed **annually** and after any significant cyber incident or system change. Oversight is provided by the Headteacher and Deputy Head (IT Co-ordinator).	✅ **Meets standard**
2. Protect against cyber attacks	Appropriate technical protections must be in place (firewalls, filtering, monitoring, malware protection).	All devices connected to the school network are protected by the **NetSweeper firewall**, managed via the ICT Service. Filtering and monitoring are applied at **multiple levels** depending on whether the user is a member of staff or a pupil. Anti-malware and security protections are enabled on all school devices.	✅ **Meets standard**
3. Secure user accounts and access	Schools must control user access, apply least-privilege principles and use MFA where appropriate.	All users have **individual accounts**. Access to shared drives and systems is granted on a **least-privilege basis**. From **January 2026**, **all staff Google and email accounts use 2FA/MFA**, enforced by the Deputy Head (IT Co-ordinator). Accounts are disabled promptly when staff leave.	✅ **Meets standard**

4. Use strong authentication (MFA)	MFA should be used for staff accounts, particularly where sensitive data is accessed.	All staff use an **authenticator app** for MFA. Authentication is **automatically requested when devices are off the school network**, while trusted on-site connections are recognised. Accounts are locked after a **two-week grace period** if MFA is not enabled. Email re-authentication is enforced every **14 days**.	✅ **Meets standard**
5. Control devices and networks	Only authorised and secure devices should connect to the school network.	**Only school-owned hardware** is permitted to connect to the school network. Devices from trusted external agencies may be approved **only at the discretion of the Headteacher**. **Personal devices** belonging to staff, parents or pupils are **not permitted** to access the network.	✅ **Meets standard**
6. Keep software and systems secure and up to date	Systems should be licensed, supported and patched regularly.	All teacher laptops run the **latest supported version of Windows**, are **fully licensed**, and receive **automatic security updates and patches** through Microsoft. Unsupported or unpatched systems are not permitted.	✅ **Meets standard**
7. Protect data and manage sharing	Access to data must be restricted, and sharing controlled to prevent data loss or breaches.	Shared drives are managed by the **Headteacher and Deputy Head (IT Co-ordinator)**. By default, drives are **not accessible outside the school**. Folder-level sharing is disabled to prevent accidental exposure. A dedicated **Planning Drive** contains no confidential data and is used to	✅ **Meets standard**

		share resources via Google Classroom.	
8. Back up important data	Schools should back up data and regularly review backup arrangements.	School data is backed up in line with ICT Service procedures. Backup arrangements are reviewed as part of the **annual cyber risk assessment** to ensure resilience and recovery capability.	✅ **Meets standard**
9. Prepare for and respond to cyber incidents	Schools must have a clear incident reporting and response process, including escalation where required.	All cyber incidents must be reported immediately to the **Deputy Head (IT Co-ordinator)** and **Headteacher**. Incidents are logged, investigated and escalated to external bodies (e.g. ICT Service, Local Authority, ICO) where required. Outcomes inform future risk assessments and training.	✅ **Meets standard**
10. Train users and build cyber awareness	Schools should provide regular cyber security training for staff and pupils.	**Annual cyber security training** is provided to **staff and governors**. Pupils receive age-appropriate cyber security education through the **computing curriculum**, including phishing awareness, safe password use and reporting concerns.	✅ **Meets standard**
11. Assign leadership responsibility	A senior leader should have responsibility for cyber security.	The **Headteacher** has overall accountability. The **Deputy Headteacher**, acting as **IT Co-ordinator**, has day-to-day responsibility for enforcing cyber security controls, MFA compliance, account management and liaison with ICT services.	✅ **Meets standard**