



**CAMPION SCHOOL**

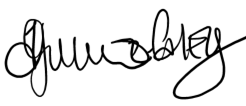
**INFORMATION SECURITY & CYBER  
SECURITY POLICY**

**Academic Year 2026–2027**



## CAMPION SCHOOL

# INFORMATION SECURITY & CYBER SECURITY POLICY

|                |                                                                                      |
|----------------|--------------------------------------------------------------------------------------|
| Policy owner   | Jassa Panesar / Robert Strain (DPO)                                                  |
| Approved by    | Governing Body                                                                       |
|                |  |
|                | Chair of Governors (Signature)                                                       |
|                |  |
|                | Headteacher (Signature)                                                              |
| Date approved  | September 2026                                                                       |
| Effective from | September 2026                                                                       |
| Review date    | September 2027                                                                       |

This policy replaces the November 2024 Information Security Policy. It retains the practical controls in that policy and updates them for current school cyber-security, data-protection and technology expectations.

# Document Control and Governance

---

This policy should be read alongside the school's Data Protection Policy, Acceptable Use Policy, Safeguarding and Child Protection Policy, Filtering and Monitoring arrangements, Records Retention Schedule, Business Continuity/Disaster Recovery Plan, Staff Code of Conduct and relevant supplier/data-processing agreements.

The policy is informed by the school's previous Information Security Policy and current Department for Education (DfE), Information Commissioner's Office (ICO) and National Cyber Security Centre (NCSC) guidance. The DfE's cyber-security standard is a core digital and technology standard and schools should be working towards meeting it by 2030. The DfE standard includes annual cyber-risk assessment, cyber-awareness, anti-malware/firewall controls, account and access security, keeping technology up to date, backups and cyber-attack reporting.

## 1. Purpose

Campion School is committed to protecting the confidentiality, integrity and availability of its information, systems and services. This policy establishes the responsibilities and minimum security requirements that apply to everyone who accesses or handles school information or technology.

## 2. Scope

- All employees, governors, trustees, agency and supply staff, volunteers, work-experience personnel, contractors, consultants and other individuals working for or on behalf of the school.
- All school information, whether paper, electronic, photographic, audio, video or verbal.
- All school-owned or school-managed devices, networks, accounts, applications and cloud services, and any personally owned device only where the school has expressly authorised access.
- Third-party providers and processors to the extent required by contract and applicable law.

## 3. Roles and Responsibilities

### 3.1 Governing Body

- Provides strategic oversight of information and cyber security;
- ensures appropriate resources, risk management and assurance arrangements are in place;
- receives appropriate assurance on significant cyber and information-security risks.

### 3.2 Headteacher and Senior Leadership Team

- Promote a whole-school security culture;
- ensure cyber security is treated as a shared responsibility, not solely an IT function;
- ensure significant risks and incidents are escalated and managed.

### **3.3 Data Protection Officer**

- The Data Protection Officer is an independent advisory and monitoring role and does not assume responsibility for the school's day-to-day information-security or IT operations.
- Operational responsibility remains with the school and its designated staff."

### **3.4 IT / Technical Support**

- Maintains appropriate technical controls, security updates, anti-malware and firewall protections;
- manages accounts, privileged access, backups, monitoring and recovery arrangements;
- supports incident response and maintains appropriate technical records.

### **3.5 All Users**

- Follow this policy and related procedures;
- protect credentials and devices;
- report suspected incidents immediately or no later than 24 hours;
- complete required security and data-protection training;
- use school systems only for authorised purposes.

## **4. Information Security Principles**

- Lawfulness, fairness and transparency.
- Purpose limitation.
- Data minimisation.
- Accuracy.
- Storage limitation.
- Integrity and confidentiality.
- Availability and resilience of critical information and systems.
- Accountability: the school must be able to demonstrate appropriate controls and governance.

## **5. Information Classification**

Information should be handled according to its sensitivity and the potential harm arising from unauthorised access, disclosure, alteration or loss.

- Public – information approved for public release.
- Internal – routine school information intended for authorised school use.
- Confidential – information where unauthorised disclosure could cause harm, including most pupil, parent and staff personal data.
- Highly Confidential / Restricted – information requiring enhanced controls, such as safeguarding, special category data, highly sensitive HR matters, credentials, security information and information whose disclosure could cause significant harm.

The school should maintain a separate information-classification guide and ensure staff understand how classification affects storage, sharing, access and disposal.

## **6. Clear Desk and Clear Screen**

- Confidential information must not be left visible or unattended.
- Paper records must be secured in locked storage when not in use.
- Confidential printouts must be collected promptly and disposed of through confidential waste arrangements.
- Devices must be locked whenever unattended.
- Screens should be positioned to prevent unauthorised viewing by pupils, visitors or members of the public.
- Staff should take care to prevent confidential conversations being overheard.

## **7. Creating, Storing and Disposing of Information**

- Confidential information must be stored only on school-approved systems or devices with appropriate access controls.
- Confidential information must not be stored on unencrypted local drives or unapproved cloud services.
- Personal email accounts must not be used as a storage or transfer mechanism for school information.
- Information must be retained in accordance with the school's Records Retention Schedule.
- Information must be securely destroyed when its retention period expires and there is no legal, regulatory or operational reason to retain it.

## **8. Email, Messaging and Information Sharing**

- Check recipients carefully before sending messages, particularly where names are similar.
- Use BCC for appropriate bulk external mailings where recipients should not see one another's addresses.
- Do not disclose personal or confidential information through ordinary messaging channels unless the channel is approved and appropriate.
- Do not click suspicious links, open unexpected attachments or provide credentials in response to unsolicited requests.
- Where sensitive information must be shared externally, use an approved secure method and verify the recipient.
- Information sharing with external organisations must have an appropriate lawful basis and, where required, a data-sharing agreement or contractual arrangement.

## **9. Passwords and Multi-Factor Authentication**

- Passwords and authentication credentials must never be shared.
- Passwords must be sufficiently long, unique and difficult to guess; users should use approved password-management facilities where provided.
- School passwords must not be reused for personal services.
- Multi-factor authentication (MFA) must be enabled where technically available, particularly for privileged, administrative, remote-access and cloud accounts.

- Users must report suspected credential compromise immediately and reset credentials where instructed.
- Administrative accounts should be separate from ordinary user accounts where technically feasible.

## **10. Access Control**

- Access must be based on an authorised business or educational need and least privilege.
- Users must not attempt to bypass permissions or access information outside their role.
- Access rights should be reviewed periodically and when roles change.
- Privileged access must be limited to authorised personnel and protected by enhanced controls, including MFA where available.
- Generic or shared accounts should be avoided unless there is a documented operational requirement and appropriate compensating controls.

## **11. Joiners, Movers and Leavers**

- New users must receive only the access required for their role.
- When staff change role, obsolete permissions must be removed and new access approved.
- Leaver accounts must be disabled promptly in accordance with the school's leaver process.
- School devices, keys, ID cards and other security items must be recovered.
- Remote access and third-party accounts must be removed or transferred as appropriate.
- Where necessary, shared credentials or service credentials must be changed following departure.

## **12. Cyber Security Controls**

- The school will maintain an annual cyber-risk assessment and review cyber risks at least termly.
- Security controls will be proportionate to identified risks and the school's technical environment.
- Anti-malware and firewall protections must be maintained and not disabled by users.
- Security updates and vulnerability fixes must be applied within appropriate risk-based timescales.
- Only authorised software and services may be installed or connected to school systems.
- Technical security controls must be tested and reviewed periodically.
- The school will maintain arrangements for cyber-attack detection, containment, recovery and learning.

## **13. Phishing, Social Engineering and Ransomware**

- Staff must remain alert to phishing, impersonation, social engineering and fraudulent payment requests.
- Unexpected requests for passwords, MFA approval, financial transfers, gift cards or sensitive information must be independently verified.
- Staff must report suspicious messages even if they have clicked a link, opened an attachment or disclosed information.
- Suspected malware or ransomware must be reported immediately; users should not attempt to investigate or remediate beyond their training.
- Where ransomware is suspected, affected devices should be disconnected from networks where safe to do so and the IT technicians must be contacted immediately.

## **14. Backups, Business Continuity and Recovery**

- The school will maintain a documented backup and recovery plan for critical systems and information.
- Backups must be protected against unauthorised access, alteration and ransomware, with segregation or immutability used where appropriate.
- Access to backup systems must be restricted and protected by strong authentication.
- Backups must have defined retention periods and be monitored for successful completion.
- Restoration tests must be conducted periodically and at least annually for critical services.
- Cyber-incident recovery arrangements must align with the school's Business Continuity and Disaster Recovery Plan.

## **15. Mobile Working and Remote Access**

- Only school-issued or explicitly authorised devices may be used to access confidential school information.
- Devices must use appropriate encryption, screen locking and security updates.
- Staff must not leave confidential documents or school devices unsecured in vehicles or public places.
- Home working must prevent access by family members or other unauthorised people.
- Public or insecure Wi-Fi should not be used for sensitive activity unless an approved secure connection is in place.
- Staff must not permanently retain work-related confidential information at home.

## **16. Removable Media**

- Removable media should be avoided where secure cloud or network storage is available.
- Only school-approved removable media may be used for storing school information.
- Confidential information stored on removable media must be encrypted.
- Removable media must not be used as the primary long-term storage location.
- Unknown or personal USB devices must not be connected to school systems unless authorised.

## **17. Mobile Phones, Photography and Video**

- Photography and video involving pupils or staff must comply with school policy, safeguarding requirements and the lawful basis for processing.
- School information must not be transferred to personal devices unless explicitly authorised.
- Images and recordings containing personal data must be stored only on approved systems and retained in accordance with the retention schedule.
- Lost devices containing school information must be reported immediately.

## **18. Generative AI and Emerging Technology**

- Staff must not enter personal, special category, safeguarding, confidential or restricted school information into publicly available generative AI tools unless the school has approved the tool and appropriate safeguards are in place.

- AI tools must be assessed for privacy, security, contractual, safeguarding and educational risks before adoption.
- Staff must not upload pupil work, staff records, safeguarding records, confidential correspondence or other restricted material to unapproved AI services.
- AI-generated content must be checked by a responsible member of staff for accuracy, appropriateness, bias and unintended disclosure before use.
- Where AI is used to process personal data, the school must consider data-protection-by-design requirements and whether a DPIA or other assessment is required.

## **19. Cloud Services and Educational Technology**

- Only school-approved cloud and EdTech services may be used for school information.
- Before procurement or significant use, the school should assess security, privacy, data location, retention, deletion, subcontractors, international transfers and contractual safeguards.
- Where a supplier processes personal data on behalf of the school, an appropriate data-processing agreement must be in place.
- Supplier access must be limited, monitored and removed when no longer required.
- Security incidents affecting school data must be reported to the school promptly in accordance with contractual requirements.

## **20. Physical and Premises Security**

- Staff must wear or display required identification on school premises.
- Visitors and contractors must sign in, display appropriate identification and be supervised in restricted areas.
- Staff should challenge or report individuals who appear to be in secure areas without authorisation, in accordance with safeguarding procedures.
- Sensitive paper and electronic records must be protected against theft, loss, fire, water damage and unauthorised access.
- Security arrangements should be reviewed through appropriate risk assessments.

## **21. Monitoring, Logging and Filtering**

- The school may monitor use of its systems and networks where lawful, proportionate and necessary for security, safeguarding, compliance and operational purposes.
- Security logs should be retained for an appropriate period and access to logs restricted.
- Monitoring arrangements must be transparent and communicated through relevant privacy notices and policies.
- Filtering and monitoring arrangements must operate in accordance with the school's safeguarding requirements and the DfE filtering and monitoring standard.
- Suspicious activity identified through monitoring must be escalated through the incident-management process.

## **22. Data Protection, Privacy and DPIAs**

- Personal data must be processed in accordance with UK data-protection law, including the UK GDPR, Data Protection Act 2018 and relevant provisions introduced by the Data (Use and Access) Act 2025.
- Processing must have an appropriate lawful basis and comply with the principles of data protection.
- Data protection by design and by default must be considered when introducing new systems, processes or technologies.
- A Data Protection Impact Assessment should be completed where required, particularly for processing likely to result in a high risk to individuals.
- Children's personal data requires particular care and appropriate safeguards.

## **23. Information Security Incidents and Personal Data Breaches**

All suspected information-security incidents must be reported immediately or no later than 24 hours through the school's approved incident-reporting route. Staff should report an incident even where they are unsure whether a breach has occurred.

1. Report the incident immediately or no later than 24 hours to the appropriate school contact/IT technicians and, where personal data may be involved, the DPO or designated data-protection contact.
2. Contain the incident where safe and within the user's competence. Do not delete evidence or attempt unsupported technical investigation.
3. Record what happened, when it happened, what information or systems may be affected and who may be affected.
4. The school will assess severity, risk and whether external notification is required.
5. Where a personal-data breach is likely to result in a risk to individuals' rights and freedoms, the school will consider ICO notification without undue delay and, where required, within 72 hours of becoming aware of the breach.
6. The school will consider whether affected individuals, the police, DfE, suppliers, insurers or other bodies need to be informed.
7. Following significant incidents, the school will review lessons learned and implement corrective actions.

## **24. Staff Training and Awareness**

- All staff and relevant governors/contractors must complete information-security and data-protection awareness training on induction and at least annually thereafter.
- Training should cover phishing, passwords and MFA, secure handling of information, AI, remote working, incident reporting and safeguarding implications.
- Cyber-awareness activity should be refreshed during the year and targeted where risk indicates.
- Training completion should be recorded and monitored.

## **25. Compliance and Disciplinary Action**

Failure to comply with this policy may expose pupils, staff and the school to significant risk and may constitute a disciplinary matter. Deliberate misuse, unauthorised access, intentional introduction of

malware, deliberate disclosure of confidential information or attempts to circumvent security controls may be treated as serious misconduct, subject to the school's disciplinary procedures.

## **26. Review, Assurance and Continuous Improvement**

- This policy will be reviewed at least annually.
- The school will review the policy following significant incidents, changes to legislation, major technology changes or changes to DfE/ICO/NCSC expectations.
- Cyber-risk assessments should be reviewed termly.
- Technical controls, access rights, backups and incident procedures should be tested or audited periodically.
- Findings from incidents, exercises, audits and training should inform future improvements.

# Appendix 1 – Staff Quick Reference: What Do I Do?

---

| Situation                                       | Immediate action                                                                                                               |
|-------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| Sent personal data to the wrong person          | Report immediately or no later than 24 hours to the DPO/data-protection contact. Do not attempt to conceal or delete evidence. |
| Clicked a suspicious link                       | Report immediately to IT. If instructed, disconnect the device from the network. Change credentials if required.               |
| Received a suspicious MFA prompt                | Do not approve it. Report it to IT/security.                                                                                   |
| Lost a laptop/phone/USB                         | Report immediately to IT and the appropriate school manager/DPO.                                                               |
| Suspect ransomware                              | Stop using the device, disconnect from the network where safe, and contact IT immediately.                                     |
| Accidentally disclosed confidential information | Report immediately or no later than 24 hours. Early reporting may allow the school to contain the incident.                    |
| Want to use a new AI or EdTech tool             | Do not upload school/pupil/staff information until the tool has been approved and relevant privacy/security checks completed.  |
| Need to send sensitive information externally   | Verify the recipient and use an approved secure sharing method.                                                                |

# Appendix 2 – Minimum Security Expectations

---

- Use only approved systems and software.
- Use MFA wherever provided.
- Never share passwords.
- Lock your screen whenever unattended.
- Check recipients before sending information.
- Do not put confidential information into unapproved AI tools.
- Keep devices physically secure.
- Report incidents immediately or no later than 24 hours, even if you are unsure.
- Complete required annual security and data-protection training.
- Follow the school's retention, disposal and information-sharing procedures.

# Appendix 3 – Related Documents and Guidance

---

- Champion School Data Protection Policy.
- Champion School Acceptable Use Policy.
- Champion School Safeguarding and Child Protection Policy.
- Champion School Records Retention Schedule.
- Champion School Business Continuity and Disaster Recovery Plan.
- Champion School Filtering and Monitoring arrangements.
- Champion School Staff Code of Conduct.
- Department for Education: Meeting digital and technology standards in schools and colleges.
- Department for Education: Data protection in schools.
- Information Commissioner’s Office: Data protection and accountability guidance.
- National Cyber Security Centre: cyber security guidance for education and organisations.

# Approval and Review Record

---

| Date           | Version | Approved by    | Notes                                      |
|----------------|---------|----------------|--------------------------------------------|
| September 2026 | 1.0     | Governing Body | New policy replacing November 2024 version |