



#equippedforlife

The
Westgate School

CYBER SECURITY POLICY

School	The Westgate School
Policy owner	Headteacher / SLT Digital Lead
Date revised	September 2026
Next review	September 2027, or sooner following significant legislative, DfE/NCSC guidance or cyber-risk changes

1. Introduction and statement of intent	3
2. Purpose and scope.....	3
3. Legal and statutory framework	3
4. Governance and responsibilities	4
4.1 Governing Board	4
4.2 Headteacher and SLT Digital Lead.....	4
4.3 IT Manager / IT Support.....	4
4.4 Designated Safeguarding Lead (DSL)	4
4.5 Data Protection Officer (DPO)	4
4.6 All users	4
5. Cyber risk assessment and assurance.....	5
6. User accounts, passwords and access control	5
7. Devices, networks, malware and firewalls.....	5
8. Software, vulnerability management and security updates	6
9. Removable media and data transfer	6
10. Backups, resilience and recovery.....	6
11. Filtering, monitoring and safeguarding	7
12. Generative AI and emerging technology	7
13. Third-party suppliers and cloud services	8
14. Cyber awareness and training.....	8
15. Acceptable use and staff responsibilities	8
16. Cyber incident management and reporting	9
16.1 Immediate response	9
16.2 External reporting.....	9
17. Personal data breaches.....	10
18. Examination and awarding-body systems.....	10
19. Monitoring, review and compliance	10
20. Related policies and plans.....	10

1. Introduction and statement of intent

Cyber security is an operational, data-protection and safeguarding responsibility. The Westgate School will protect its pupils, staff, systems, services and information from unauthorised access, loss, disclosure, alteration, disruption and cyber attack.

The school recognises that a cyber incident can prevent access to safeguarding information, expose sensitive information about children, disrupt teaching and school operations, cause financial loss and create direct risks to pupils and staff. Cyber security is therefore not solely an IT function; it is a whole-school responsibility.

This policy replaces the September 2024 Cyber Security Policy and should be read alongside the school's Child Protection and Safeguarding Policy, Data Protection Policy, Data Breach Policy, Information Security Policy, Acceptable Use Policy, Online Safety arrangements, Business Continuity/Disaster Recovery Plan and relevant staff codes of conduct.

2. Purpose and scope

This policy establishes the governance, technical controls, staff expectations, training, risk-management and incident-response arrangements used by the school to reduce cyber risk and respond effectively to incidents.

It applies to governors, employees, agency and supply staff, volunteers, contractors, pupils and any other person who is given access to the school's network, systems, data or digital services. It applies to school-owned devices and services and, where authorised, to personal devices used to access school systems.

3. Legal and statutory framework

This policy has regard to current legislation and statutory or official guidance applicable to schools in England, including:

- Keeping Children Safe in Education (KCSIE) 2026, including the requirement for appropriate filtering and monitoring and the recognition that secure information systems form part of effective safeguarding practice.
- UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, as amended.
- The Data (Use and Access) Act 2025, including data-protection changes brought into force in 2026.
- Computer Misuse Act 1990.
- Human Rights Act 1998 and Equality Act 2010 where relevant to monitoring, access and the use of technology.
- Department for Education (DfE) Digital and Technology Standards for Schools and Colleges, including the Cyber Security core standard and Filtering and Monitoring core standard, updated September 2026.
- National Cyber Security Centre (NCSC) guidance for schools and current Cyber Essentials technical principles where applicable.

Where legislation, statutory guidance or mandatory DfE requirements change, the school will update its procedures without waiting for the next scheduled policy review.

4. Governance and responsibilities

4.1 Governing Board

- Provide strategic oversight of cyber security as a school risk and receive assurance that identified risks are being managed.
- Ensure that cyber security, safeguarding, data protection and business continuity arrangements are appropriately linked.
- Ensure that at least one current governor/trustee undertakes appropriate cyber-security awareness training.
- Receive notification of significant cyber incidents and assurance about remedial actions.

4.2 Headteacher and SLT Digital Lead

- The Headteacher is accountable for ensuring that appropriate cyber-security arrangements are in place.
- A designated SLT Digital Lead will coordinate cyber-security strategy, risk assessment, training, incident response and compliance with DfE standards.
- Cyber risks will be included in the school risk-management process and significant risks escalated to governors.

4.3 IT Manager / IT Support

- Implement and maintain the technical controls required by this policy and current DfE standards.
- Maintain network, hardware, software, cloud-service and configuration documentation.
- Monitor systems for suspicious activity and respond promptly to alerts, vulnerabilities and incidents.
- Maintain appropriate asset, software, account and access records.

4.4 Designated Safeguarding Lead (DSL)

The DSL will advise on safeguarding requirements relating to systems, filtering and monitoring, cyber incidents and the protection and availability of child-protection information. Any cyber incident that creates a safeguarding risk will be managed jointly through safeguarding and cyber-incident procedures.

4.5 Data Protection Officer (DPO)

The DPO will advise on privacy, data-processing risks, Data Protection Impact Assessments (DPIAs), personal-data breaches and statutory reporting to the Information Commissioner's Office (ICO).

4.6 All users

All users are responsible for following this policy, protecting credentials and devices, completing required training and immediately reporting suspected cyber incidents, phishing, data loss, unusual system behaviour or mistakes that may create a security risk.

5. Cyber risk assessment and assurance

- A documented cyber risk assessment will be completed at least annually and following a significant incident, major technology change or material change in risk.
- The risk assessment will be revisited at least termly to identify changes in threats, vulnerabilities, systems, suppliers or user behaviour.
- The assessment will consider safeguarding data, personal data, finance systems, MIS, communications, examination systems, cloud services, physical security of infrastructure, remote access and third-party suppliers.
- The school will maintain an incident-response plan and ensure cyber risks and recovery arrangements are incorporated into business continuity and disaster recovery planning.
- Critical cyber and business-continuity documentation will be accessible from a secure alternative location if normal systems are unavailable.

6. User accounts, passwords and access control

- Every user will have unique credentials. Shared accounts will be avoided except where technically necessary and formally authorised.
- Access will follow the principle of least privilege: users will only have access to systems and information required for their role.
- Accounts will be created only when required and disabled promptly when a user leaves or no longer requires access.
- Joiner, mover and leaver processes will be coordinated between IT, HR/business support and relevant leaders.
- User accounts and access rights will be reviewed at least termly.
- Privileged or administrative accounts will be separate from normal day-to-day accounts and will not be used for routine email or web activity.
- Password strength will be enforced technically. Compromised or suspected-compromised passwords must be changed immediately.
- Multi-factor authentication (MFA) must be enabled for staff accounts accessing cloud services or remotely accessing on-site systems, and for IT administrative accounts, where the service supports it. Enhanced authentication will be used for access to confidential or sensitive information.
- Remote access will be enabled only where required and authorised, and disabled when no longer needed.

7. Devices, networks, malware and firewalls

- All network-connected devices, including Internet of Things (IoT) devices, will be securely configured, supported and kept up to date.
- The school will use correctly configured boundary firewalls and appropriate software firewalls. Firewall firmware, rules and permitted inbound connections will be reviewed at least termly.

- Anti-malware protection, including anti-virus, will be centrally managed, actively monitored and kept up to date on applicable devices and managed servers.
- Systems will be configured to reduce the spread of malware between devices and critical systems.
- IT will monitor alerts and logs appropriate to the school's risk profile and investigate suspicious activity.
- Default administrator credentials will be changed before equipment is put into service.
- Unauthorised attempts to bypass firewalls, filtering, monitoring, anti-malware, browser controls or other security measures are prohibited.

8. Software, vulnerability management and security updates

- Only licensed, supported and authorised software, applications, browser extensions and cloud services may be used for school business.
- IT will maintain records of software, licensing and end-of-support dates and will remove or isolate unsupported technology.
- Critical/high-risk vulnerability fixes for operating systems, applications and firmware will be completed within 14 days of the fix being released where required by the DfE cyber-security standard.
- Where the DfE issues a specific security-update instruction, IT will apply the update within the timeframe specified by the DfE; current guidance expects action within 5 working days of notification.
- Where a high-risk vulnerability cannot be fixed promptly, affected devices or services will be isolated or otherwise mitigated until the risk is acceptably controlled.
- New applications and cloud services will be security-checked before approval, and a DPIA will be completed where required.

9. Removable media and data transfer

- USB and other removable storage will be prohibited by default unless there is an identified and authorised operational need, for example an examination-board requirement.
- Permitted removable media must be scanned for malware before use and must be encrypted where it contains personal, confidential or sensitive information.
- Personal data must not be transferred through unapproved personal email accounts, consumer file-sharing services or unauthorised applications.
- Physical backups or storage containing school data must not be taken to a person's home.

10. Backups, resilience and recovery

- The school will maintain a documented backup and recovery plan, owned by the SLT Digital Lead and implemented by IT support.

- Important data will have at least three backup copies across at least two separate devices or services, with at least one copy held off-site.
- Backups will be designed to resist ransomware and, wherever technically possible, will be immutable so that completed backups cannot be altered.
- Backups will be tested and logged at least termly, including restoration tests, and the backup plan will be reviewed at least annually and after significant system changes.
- Recovery priorities will include safeguarding and child-protection information, MIS/attendance, communications, finance and other systems required to operate the school safely.
- Backup retention will align with statutory duties and the school's records-retention requirements.

11. Filtering, monitoring and safeguarding

The school will maintain filtering and monitoring arrangements that meet KCSIE 2026 and the DfE Filtering and Monitoring core standard. These arrangements are safeguarding controls as well as technical controls.

- Roles and responsibilities for filtering and monitoring will be clearly assigned.
- Harmful and inappropriate content will be blocked without unreasonably restricting teaching and learning.
- Effective monitoring strategies will be used to identify safeguarding and security concerns.
- The effectiveness of filtering and monitoring will be reviewed at least annually and checks will include internet-connected devices in relevant locations.
- The DSL, SLT Digital Lead and IT support will work together on filtering and monitoring risks and responses.
- Cyber-security controls and filtering/monitoring arrangements will take account of risks associated with generative artificial intelligence (AI), including malicious content, data leakage, unsafe services and attempts to bypass security controls.

12. Generative AI and emerging technology

- Staff and pupils must only use AI tools and other emerging technologies in accordance with school-approved arrangements.
- Personal, safeguarding, confidential or special-category data must not be entered into public or unapproved generative-AI systems.
- New AI-enabled products will be assessed for security, privacy, safeguarding and supplier risk before adoption.
- The school will consider whether AI-enabled services create new risks to filtering, monitoring, authentication, data retention, intellectual property or information accuracy.
- Where AI tools process personal data, the DPO will be consulted and a Data Protection Impact Assessment (DPIA) completed where required.

13. Third-party suppliers and cloud services

- Cyber-security and data-protection risks will be considered when procuring or renewing digital services.
- Suppliers that process school data will be subject to appropriate due diligence, contractual controls and data-processing arrangements.
- The school will consider supplier security, access controls, MFA, patching, backups, incident notification, business continuity, data location and exit arrangements.
- Where IT support is outsourced, the provider will be expected to demonstrate how it meets the school's required DfE cyber-security standards and how risks from the provider's own systems are controlled.

14. Cyber awareness and training

- The school will maintain a cyber-awareness plan for staff and pupils.
- Cyber-security training will be completed at least annually by staff and will be refreshed sooner where risks change or an incident identifies a training need.
- Training will cover phishing and social engineering, password security, MFA, online safety, physical device security, removable media, incident reporting and personal-data breaches.
- Age-appropriate cyber awareness will be provided to pupils through the curriculum and wider online-safety education.
- At least one current governor/trustee will undertake appropriate cyber-security training.
- Supply staff, agency workers, contractors and others with school logins will receive appropriate security information or training as soon as practicable.
- Where the school is covered by the DfE Risk Protection Arrangement (RPA), it will retain evidence of any cyber-training requirements that are conditions of cover.

15. Acceptable use and staff responsibilities

The school's Acceptable Use Policy applies to all authorised users. In addition, staff must:

- keep passwords and authentication methods secure and never approve an Multi-Factor Authorisation (MFA) request they did not initiate;
- lock devices when unattended and protect devices from loss or theft;
- not share accounts or allow another person to use their credentials;
- not disable, alter or circumvent security, filtering or monitoring controls;
- not install software, applications or browser extensions without IT approval;
- use only approved systems for school information and communications;
- remain alert to phishing, unexpected attachments, QR-code scams, fraudulent payment requests and social-engineering attempts;
- report lost devices, suspicious messages, accidental disclosures and security mistakes immediately;

- not use personal devices to access school systems unless this has been expressly authorised and appropriate technical controls are in place.

Deliberate or negligent misuse of school systems may be dealt with under the school's disciplinary, behaviour or safeguarding procedures as appropriate.

16. Cyber incident management and reporting

Any suspected cyber incident, attack, compromise or near miss must be reported immediately to IT support and the SLT Digital Lead. Staff must not delay reporting while attempting to investigate the matter themselves.

16.1 Immediate response

- Activate the cyber incident response plan and relevant business-continuity arrangements.
- Contain the risk, isolate affected systems where necessary and preserve evidence.
- Assess the effect on safeguarding, teaching, operations, personal data, examinations and finance.
- Inform the Headteacher, DPO and DSL as appropriate and notify governors of significant incidents.
- Record incidents, attacks and near misses and document decisions and actions.

16.2 External reporting

Where appropriate, an authorised senior leader will coordinate external reporting. Depending on the circumstances, this may include:

- the school's Risk Protection Arrangement (RPA) or cyber-insurance provider;
- Report Fraud, using the current national fraud and cyber-crime reporting arrangements;
- the DfE Sector Cyber Team at Sector.Incidentreporting@education.gov.uk;
- the National Cyber Security Centre (NCSC), particularly for serious incidents causing major or prolonged disruption or serious financial damage;
- the Information Commissioner's Office (ICO), where a personal-data breach is legally reportable, within the statutory timeframe;
- the police or other relevant agencies where criminal activity or an immediate safeguarding risk is suspected;
- relevant awarding organisations where examination or assessment systems may have been compromised.

No ransom payment or communication with a cyber-criminal will be authorised by an individual member of staff. Any such decision will be escalated immediately to the Headteacher and relevant external advisers/insurers and handled in accordance with law and government guidance.

17. Personal data breaches

Where a cyber incident involves, or may involve, a personal-data breach, the school's Data Breach Policy will be activated alongside this cyber incident process. The DPO will assess the breach, advise on containment and determine whether notification to the ICO and/or affected individuals is required.

Where compromised information includes safeguarding or child-protection information, the DSL will assess any immediate or ongoing risk to individual children and take safeguarding action without waiting for the conclusion of the technical investigation.

18. Examination and awarding-body systems

- Access to awarding-body systems will be restricted to authorised users and protected using the authentication controls required by the awarding organisation.
- MFA devices or credentials used for awarding-body systems must be kept secure and must not be shared.
- Any actual or suspected compromise of an awarding-body online system will be reported immediately to the relevant awarding organisation and managed under this policy.

19. Monitoring, review and compliance

- This policy will be reviewed at least annually and sooner following a significant cyber incident, material technology change, legislative change, or significant revision to DfE/NCSC guidance.
- The SLT Digital Lead and IT support will review progress against the DfE Cyber Security core standard and associated Digital and Technology Standards.
- Termly assurance will include, as appropriate, review of cyber risks, user accounts and privileges, firewall arrangements, anti-malware status, backups/restoration testing, supported software and outstanding vulnerabilities.
- The Governing Board will receive appropriate assurance that cyber risks are being identified and managed.

20. Related policies and plans

- Child Protection and Safeguarding Policy
- Data Protection Policy
- Data Breach Policy
- Information Security Policy
- Acceptable Use Policy
- Online Safety / Filtering and Monitoring arrangements
- Business Continuity and Disaster Recovery Plan
- Staff Code of Conduct
- Behaviour and Engagement Policy
- Examinations policies and procedures