CYBER SECURITY POLICY

Tonbridge School is committed to safeguarding its information assets, IT systems, and the personal data of students, staff, parents, and external stakeholders from cyber threats. This Cyber Security Policy outlines the School's approach to cyber defence, defines roles and responsibilities, and ensures compliance with relevant legislation, including the Data Protection Act 2018, UK GDPR, the Computer Misuse Act 1990, and guidance from the Department for Education (DfE), National Cyber Security Centre (NCSC), and JCQ.

This policy should be read in conjunction with the following policies:

- IT Acceptable Use Policy (Staff)
- Acceptable Use of Computers Policy (Boys)
- Online Safety Policy
- Emerging Technology and AI Policy
- Data Protection Policy

This policy applies to all staff, pupils, governors, contractors, and third parties with access to Tonbridge School's IT systems, digital services, or data, whether using school devices or personal devices connected to the school's network.

Roles and Responsibilities

All users of the school's IT, Wi-Fi and digital services are expected to use systems responsibly and report any concerns to the Director of IT & Digital, who holds strategic oversight of cybersecurity across the school. Operational responsibility for implementing cyber defence measures lies with the IT Infrastructure and Operations team, acting under the direction of the Director of IT & Digital.

The Deputy Head Academic, as the Head of Centre, is responsible for supporting the implementation of this policy in line with JCQ regulations and centre compliance requirements. The Head of Centre and Exams Officer retain accountability for ensuring that awarding organisation systems are accessed only by authorised personnel.

All staff and pupils must be familiar with this policy and adhere to it.

Incident Response Plan

Staff must report any suspected cyber incidents by emailing ithelp@tonbridge-school.org or contacting the Director of IT & Digital directly.

Response Process:

1. The Director of IT & Digital will lead the initial response, delegating investigation and containment actions to the Infrastructure team.
2. The Incident Response Team will be convened if the issue is significant.
3. The DPO and DSL will be notified where safeguarding or data protection concerns arise.
4. Relevant external authorities (e.g. NCSC, Police, JCQ, DfE, ICO) will be contacted where appropriate.
5. The incident, mitigation steps and outcomes will be documented securely.
6. A post-incident review will take place within 10 working days.

Technical Security Measures

The school implements the following measures in line with NCSC and DfE guidance:

- Next-generation firewall and web content filtering
- Anti-virus/anti-malware on all endpoints
- Managed Detection and Response (MDR) solution across the network and resources
- Microsoft 365 with MFA enabled for all users (students and staff)
- Entra ID and Azure AD for identity management
- Regular system patching and secure configuration
- Secure cloud use (Microsoft 365, SharePoint, OneDrive, Teams)
- Automated and encrypted backups with tested restore procedures
- Centralised logging and audit trails
- Prompt removal of access for leavers
- Device encryption and secure disposal protocols

User Account Management

- User access is role-based and reviewed upon changes in employment or responsibilities
- Passwords must never be shared, reused across systems, or stored insecurely
- Staff are advised not to use personal passwords for school systems
- In line with NCSC guidance, routine password expiry is not enforced unless there is a suspicion of compromise
- Microsoft 365 Multi-Factor Authentication (MFA) is mandatory for all staff and students
- User accounts are disabled immediately when an individual leaves the organisation or no longer requires access
- Administrative privileges are limited to authorised staff and reviewed regularly
- Account activity is monitored through audit logs and anomaly detection systems, with automatic alerts generated by Microsoft 365 Security

Staff Training and Awareness

- All teaching and support staff with a standard or full school account (i.e., one that includes external email access) must complete the NCSC 'Cyber Security Training for School Staff' annually, accessed via SecureSchools.com.
- Staff who access awarding bodies' online systems (e.g. AQA, Pearson, OCR portals) are additionally required to download and retain their certificate of completion, which must be available for inspection in line with JCQ General Regulations 3.21(a).
- Completion certificates are retained digitally and made available to the Head of Centre and Exams Officer
- Additional phishing and social engineering training is integrated into wider safeguarding and IT onboarding

Compliance and Auditing

- This policy will be reviewed annually by the Head of Centre and the Director of IT & Digital, and ratified by the Second Master
- Internal security posture audits are conducted annually
- External penetration testing is continuous (external-to-internal) and quarterly (internal)
- SecureSchools training records are retained in line with JCQ inspection requirements

Third-Party Risk and Supply Chain Security

All third-party systems that store or process school data must meet minimum security standards in line with UK GDPR. The Director of IT & Digital is responsible for ensuring that systems such as PASS, Firefly, and CPOMS are subject to appropriate vendor due diligence, including data protection impact assessments where required.

Risk Mitigation Strategy & Cyber Insurance

Tonbridge School holds appropriate cyber insurance and contracts with a Third-Party Response service to ensure 24/7 threat monitoring and rapid incident response (MDR). These measures form part of our risk mitigation approach.

Review and Approval

This policy will be reviewed annually in October or following a significant incident, change in infrastructure, or legal update.