BORDEN GRAMMAR SCHOOL



Cybersecurity Policy

Review Responsibility:	Network Manager
Frequency of Review:	1 year
Date Approved:	Nov 26
Approved By:	Board of Trustees
Next Review Due By:	Nov 27

Contents

1. Purpose and Scope **3**

2. Roles and Responsibilities **3**

Board of Trustees 3

Headteacher 3

Designated Safeguarding Lead (DSL) 3

Data Protection Officer (DPO) 3

IT Department 3

All Users 3

3. Governance and Risk Management **3**

4. Technical Controls **4**

5. Accounts & Access Control **4**

6. Data Protection **4**

7. Training & Awareness **4**

8. Filtering & Monitoring **5**

9. Incident Response **5**

10. Business Continuity & Disaster Recovery **5**

11. Review **5**

1. Purpose and Scope

This policy sets out how Borden Grammar School protects its networks, systems, devices, and data from cyber threats. Cybersecurity is treated as a **safeguarding and operational continuity issue**, not solely an IT matter, consistent with the DfE's cybersecurity standards for schools and colleges and *Keeping Children Safe in Education* (KCSiE), which frames protection of personal information as part of wider safeguarding responsibilities.
This policy applies to all staff, pupils, trustees, contractors, volunteers, and third parties who access school systems, whether on-site or remotely.

2. Roles and Responsibilities

Board of Trustees

- approves this policy
- ensures it is reviewed annually
- cyber risk reported at board/audit committee level at least annually.

Headteacher/Leadership Digital Lead

- owns implementation
- coordinates the incident response plan
- reviews risk assessments

School Business Manager

- assures systems and protocols in place for IT department to follow

Designated Safeguarding Lead (DSL)

- links cyber incidents affecting safeguarding data to safeguarding processes

Data Protection Officer (DPO)

- oversees GDPR obligations, breach assessment, ICO notification.

IT Department

- day-to-day technical controls, monitoring, patching, backups
- reporting to the School Business Manager

All Users

- comply with the Online Safety & Acceptable Use Policy
- report suspected incidents immediately
- undertake relevant training

3. Governance and Risk Management

- An annual cybersecurity **risk assessment** will be conducted and maintained in an IT/cyber risk register.
- Progress against DfE digital and technology standards will be assessed, with a documented roadmap of improvement (consistent with the DfE's expectation of evidenced progress over time rather than one-off declarations of compliance).

- Insurance cover (commercial or the DfE's Risk Protection Arrangement) will be reviewed annually. Where RPA cover is held, annual completion of NCSC training by staff is a condition of cover.
- Procurement of technology will consider supplier security posture, with Cyber Essentials (Plus where appropriate) expected of suppliers under DfE/Crown Commercial Service framework expectations.

4. Technical Controls

Firewalls: All devices connected to school networks will be protected by a properly configured boundary or software firewall. Firewall rules will be reviewed at least annually.
Anti-malware: Anti-malware software will be deployed on all devices, centrally monitored, configured to scan web pages, email attachments, and downloaded files, and to alert administrators to threats.
Devices: A register of all hardware and network devices will be maintained and kept up to date, with security features enabled and configurations kept current. Devices will be enrolled in centralised management where possible.
Patching and licensing: Operating systems and software will be supported, licensed, and updated promptly. Unsupported systems will be isolated or decommissioned.
Backups: Critical data will be backed up following the 3-2-1 principle (three copies, two media, one off-site/offline), with restoration tested at least annually and backups protected from tampering (immutable or offline where feasible).
Wireless and networks: Wireless access will require secure authentication; guest networks will be segregated from the curriculum and corporate networks.

5. Accounts & Access Control

- The main areas of vulnerability at Borden are through Arbor, Google, CPOMS and FMS (financial management system) due mainly to their availability via the Internet. Security for these is handled by the relevant service provider(s) and 2 factor authentication is applied where practical.
- Any data storage systems including those containing backups of sensitive information are located in secure areas within the school and/or are encrypted to protect against data breaches due to physical theft of those devices.
- Accounts will have only the access required for the user's role (**least privilege**).
- **Multi-factor authentication (MFA)** will be enabled on all remote access, email, and privileged accounts, and wherever technically possible for all users.
- Unique named accounts will be used; shared accounts will be avoided and documented where unavoidable.
- Joiners/movers/leavers processes will ensure access is adjusted promptly; leaver accounts disabled on or before their departure date.
- Strong passwords will be enforced in line with NCSC guidance, with password managers encouraged.
- Privileged (administrator) accounts will be separate from day-to-day accounts.

6. Data Protection

- Personal data (including SEND, safeguarding, FSM, behavioural, and HR records) will be handled per UK GDPR, the Data Protection Act 2018, and the Data (Use and Access) Act 2025, as reflected in KCSiE.
- Data Protection Impact Assessments (DPIAs) will be conducted where processing presents high risk.
- Data will be encrypted at rest and in transit on portable/media devices wherever possible.

7. Training & Awareness

- All staff will complete annual cybersecurity training (NCSC "Top Tips for Staff" training satisfies the RPA condition).
- New staff will receive cybersecurity induction training as part of onboarding.
- Pupils will receive age-appropriate online safety education as part of the curriculum.
- Governors and trustees will receive periodic cybersecurity briefings.
- An up-to-date **Acceptable Use Policy** will be maintained, communicated to all users at the start of each academic year, and signed by staff and pupils.

8. Filtering & Monitoring

Appropriate filtering and monitoring (Studentkeeper, NetSupport DNA, AB Tutor and Wazuh SIEM) will be in place in line with KCSiE and the DfE filtering and monitoring standards, with the DSL involved in oversight. Monitoring covers signs of compromise (unusual logins, malware alerts) which are tracked by the ICT department. This is as well as safeguarding concerns which are monitored and tracked by the DSL for students and headteacher for staff.

9. Incident Response

A cyber incident response plan will be maintained, tested at least annually (tabletop exercise as a minimum), and included in the school's disaster recovery and business continuity plans. It will cover:

1. **Identify and contain** — isolate affected systems; do not pay ransoms or attempt recovery before containment.
2. **Notify** — the applicable routes:
    - **ICO within 72 hours** where personal data is affected
    - **Action Fraud** for financial fraud
    - **Police (101)** for criminal offences
    - **DfE Sector Cyber Team** via the Education Cyber Resilience Programme
    - **Local authority designated officer** where safeguarding data is involved
    - Parents/pupils where ICO guidance requires
    - The trust board/ESFA as part of risk reporting (academies)
3. **Recover** — restore from tested backups; validate integrity before reconnecting.
4. **Review** — lessons learned, policy updates, and reporting to trustees.

10. Business Continuity & Disaster Recovery

Digital technology will be included in disaster recovery and business continuity plans, with contingency arrangements for continued teaching and communication during prolonged system outages.

11. Review

This policy will be reviewed annually, or following any significant incident, major system change, or update to DfE/NCSC guidance.