

CYBER SECURITY POLICY

BRAMHALL HIGH SCHOOL

AUTHOR: A NORTON
REVIEW DATE: SEPTEMBER 2025
APPROVED DATE: DECEMBER 2025
NEXT REVIEW DATE: DECEMBER 2026

CONTENTS

1. Introduction, Purpose & Scope....3
   1.1. Purpose....3
   1.2. Scope....3

2. Related Policies....4

3. Roles & Responsibilities....4
   3.1. Governing Board....4
   3.2. Headteacher....5
   3.3. Operations Manager....5
   3.4. Network Manager....5
   3.5. Data Protection Officer – LEA Provided....6
   3.6. Staff....6
   3.7. Students....6

4. Cyber Security Principles....6

5. Access Control and Authentication....7

6. Network and Device Security....7
   6.1. Use of School Devices....7
   6.2. Protective Measures....8
   6.3. Monitoring and Audit....9

7. Email and Communication Security....9
   7.1. Protective Measures....9
   7.2. Use of Email....9

8. Education and Awareness....10

9. Remote Working, Remote Learning & Bring Your Own Device (BYOD)....10
   9.1. Staff Remote Working....10
   9.2. Student Remote Learning....10
   9.3. Bring Your Own Device (BYOD) 10

10. Remote Working, Remote Learning & Bring Your Own Device (BYOD)....11
   10.1. Prohibited Use....11
   10.2. Permitted Use....12
   10.3. Additional Requirements....13

11. Incident Response and Reporting....14

12. Policy Enforcement....14

1. INTRODUCTION, PURPOSE & SCOPE

Information and communication technology (ICT) is central to the operation of Bramhall High School. This policy outlines how the school will safeguard its systems, networks, and data against cyber threats, ensuring that information is protected, teaching and learning can continue uninterrupted, and the welfare of pupils and staff is not compromised.

1.1. PURPOSE

The aims of this policy are to:

- Protect the school's data, networks, and systems from unauthorised access or damage.
- Ensure the confidentiality, integrity, and availability of school information.
- Define clear roles, responsibilities and behaviours expected from all users.
- Ensure compliance with relevant legislation and good practice standards.
- Minimise disruption to teaching, learning, and administration caused by cyber incidents.
- Promote a culture of cyber awareness across the school community.

1.2. SCOPE

The policy applies to:

- All staff (teaching, support, temporary, volunteers, governors).
- All students enrolled at the school.
- Third parties, contractors, and visitors using school IT systems or accessing school data.
- All devices used to access school systems, whether owned by the school or personally, and regardless of where the school systems are accessed from.

It covers:

- All IT systems including hardware, software, and cloud services.
- Internet and email usage.
- Data storage and transfer.
- Cyber incident management and reporting.

2. RELATED POLICIES

The following policies support this cyber security policy and should be read in conjunction with it.

- Acceptable use policy
- Data protection policy
- Safeguarding policy

3. ROLES AND RESPONSIBILITIES

The following roles and responsibilities apply in respect of this policy.

3.1. GOVERNING BOARD

- Provide oversight and strategic direction for cyber security.
- Review and approve this policy annually.
- Ensure adequate funding and resources are allocated to cyber security.
- Supporting the headteacher and other relevant staff in the delivery of this policy.
- Ensuring at least one member of the board completes basic cyber-security training.

3.2. HEADTEACHER

- Hold overall accountability for the security of school systems and data.
- Ensure this policy is implemented and embedded.
- Ensure all staff members and pupils are aware of their responsibilities in relation to this policy.
- Report serious cyber security incidents to relevant authorities.

3.3. OPERATIONS MANAGER

- Monitor and review the implementation and effectiveness of this policy.
- Organise annual cyber security training for all staff members.
- Determine which organisations and individuals need to be notified following a security incident and ensuring they are notified.
- Lead the school's response to cyber security incidents, including appointing and leading the recovery team in the event of an incident.
- Maintain a cyber security risk register, reviewed termly.
- Maintain a cyber security incident management plan, reviewed termly.
- Maintain records of data breaches.

3.4 NETWORK MANAGER

- Implement and maintain technical security controls (firewalls, antivirus, patching, filtering).
- Manage user accounts, permissions, and backups, ensuring appropriate user access procedures are in place.
- Conduct security monitoring and risk assessments.
- Coordinate incident response and recovery.
- Respond to alerts for access to inappropriate content

- Ensure a log of cyber-security incidents is maintained.
- Ensure new technologies are assessed for cyber security risk prior to implementation.

3.5. DATA PROTECTION OFFICER – LEA PROVIDED

- Advise on compliance with UK GDPR.
- Oversee reporting to the Information Commissioner's Office (ICO) where required.

3.6. STAFF

- Use IT systems responsibly in line with this policy.
- Protect passwords and handle data responsibly.
- Report suspected cyber security incidents immediately.
- Complete acceptable use policy

3.7. STUDENTS

- Use technology responsibly under staff supervision.
- Follow the Acceptable Use Policy (AUP).
- Report online safety concerns or incidents to a member of staff or trusted adult.

4. CYBER SECURITY PRINCIPLES

The school adopts the NCSC's "10 Steps to Cyber Security" framework, focusing on:

- Risk management
- User education
- Access control

- Malware prevention
- Network security
- Data protection
- Incident management
- System maintenance
- Monitoring
- Home and mobile working

5. ACCESS CONTROL AND AUTHENTICATION

The following measures shall be followed:

- Every user must have a unique login ID.
- Passwords must be strong, confidential, and regularly updated. Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays).
- Multi-factor authentication (MFA) must be used wherever supported.
- Access will be limited to data necessary for the user's role ("principle of least privilege").
- Accounts for leavers will be disabled within 24 hours.

6. NETWORK AND DEVICE SECURITY

6.1. USE OF SCHOOL DEVICES.

All staff must:

- Ensure that school devices are password protected and locked when unattended.
- Avoid accessing internal systems or accounts from devices other than their allocated device, or lending their device to others.

- Log into school accounts and systems through secure and private networks only.
- Report stolen or damaged equipment as soon as possible
- Change all account passwords at once if a device is stolen.
- Report a perceived threat or possible security weakness in school systems.
- Refrain from downloading suspicious, unauthorised or illegal software on school equipment.

6.2. PROTECTIVE MEASURES

The following protective measures will be applied:

- All school devices must run up-to-date anti-virus and security software.
- Operating systems and applications must be regularly patched and updated.
- Internet access will be filtered to block harmful or inappropriate content.
- Firewalls and intrusion detection systems will protect the school's network.
- Regular backups will be performed and stored securely off-site or in a secure cloud service.
- Anti virus and malware software shall be installed on all school devices and regularly updated.
- The use of removable media (such as USB sticks) will be prohibited on school devices.
- All external providers must meet school security standards, and appropriate due diligence must be carried out before onboarding suppliers.
- Third party contracts must specify responsibilities for data protection and incident notification.

6.3. MONITORING AND AUDIT

The following measures will be applied:

- Network and system logs will be maintained and reviewed.
- External penetration testing or security audits will occur periodically and non-compliance or vulnerabilities will be addressed promptly.

7. EMAIL AND COMMUNICATION SECURITY

7.1. PROTECTIVE MEASURES

The following protective measures will be applied:

- Inbound and outbound emails will be scanned for malicious and spam content using appropriate software and automatically blocked where appropriate.
- Phishing simulations will be run periodically as part of cyber security training

7.2. USE OF EMAIL

All staff must:

- Use school provided email accounts for school business.
- Avoid opening attachments and clicking on links when the content is not adequately explained.
- Practice good email vigilance – for example, be suspicious of 'clickbait' titles (e.g. offering prizes, advice.), check email addresses and names of people they received a message from to ensure they are legitimate, look for inconsistencies.
- Ensure that the recipients of the emails are properly authorised people or organisations and have adequate security policies.
- Ensure that emails are sent to the correct email addresses/contacts and take particular care when sending mass emails (eg. via BCC facility)
- Report suspicious emails or phishing attempts to the IT helpdesk.

8. EDUCATION & AWARENESS

The following measures will be applied:

- All staff must complete cyber security training annually, covering phishing, social engineering, data protection, and online safety.
- New staff will receive induction training covering cyber security.
- Students will receive age-appropriate lessons on cyber awareness and online behaviour.
- Awareness campaigns (posters, newsletters) will reinforce key messages.
- Parents will be offered guidance on supporting online safety at home.

9. REMOTE WORKING, REMOTE LEARNING AND BRING YOUR OWN DEVICE (BYOD)

The following measures will be applied:

9.1. STAFF REMOTE WORKING

All obligations under this policy are required to be followed during periods of remote working

9.2. STUDENT REMOTE LEARNING

Remote learning must be conducted only through school-approved platforms (e.g., Microsoft Teams, Class Charts etc) Multifactor authentication should be used when required by specific applications.

9.3. BRING YOUR OWN DEVICE. (BYOD)

Access to the main school network and resources is only permitted using school issued devices whilst on school premises.

10. USE OF ARTIFICIAL INTELLIGENCE (AI) TOOLS

Artificial Intelligence (AI) tools, including generative AI platforms such as ChatGPT, Microsoft Copilot and Google Gemini, introduce significant data protection, safeguarding, and cyber security risks if used inappropriately.

The school does not currently provide or approve any AI platform for handling personal or sensitive information.

Free or consumer versions of AI tools are external services that:

- Do not guarantee privacy or confidentiality
- May store or reuse submitted information
- Are not covered by school or local authority data protection agreements
- May process data outside the UK
- May produce content that is inaccurate, biased or discriminatory, inappropriate or unsuitable.

Therefore, users must exercise extreme caution and must not use these platforms to process any personal or sensitive school-related information.

10.1. PROHIBITED USE

Under no circumstances may any user submit the following to any AI tool:

- Personal data (as defined under UK GDPR), for example:
- Staff/pupil/parent names
- Contact details
- Attendance, behaviour, safeguarding, assessment, or medical information
- Photos, videos, or audio that identify individuals
- Special category data, for example:
- Ethnicity

- SEN or health needs
- Safeguarding concerns
- Third party/copyrighted material, for example:
- Exam papers
- Textbook content
- Educational material used under licence
- Confidential school information, for example:
- Internal documents not publicly available
- Financial or HR information
- Performance information

If any user submits prohibited data, this may constitute a data breach and must be reported immediately in line with the school's breach reporting procedure.

10.2. PERMITTED USE

AI tools may be used for general, non-sensitive, non-identifiable, and non-copyrighted tasks, such as:

- Generating ideas for teaching activities or worksheets
- Producing generic text templates or explanations
- Improving grammar or readability of text you created yourself
- Creating revision prompts or quiz questions not based on copyrighted material
- Researching general, non-personal information
- Exploring creative tasks

All generated content must be:

- Fact-checked
- Age-appropriate
- Free from bias, harmful content, or misinformation
- Reviewed by staff before use with pupils

10.3. ADDITIONAL REQUIREMENTS

Pupils must:

- Only use AI tools when supervised, or when directed by a teacher
- Never enter personal information about themselves or others
- Ensure all AI use aligns with the Acceptable Use Policy
- Understand that AI content may be inaccurate, biased, or inappropriate

Teachers must actively supervise pupil use of AI where it is permitted.

All users must:

- Use AI tools critically and understand their limitations
- Not rely solely on AI for factual accuracy
- Ensure any AI-generated content complies with safeguarding and equality standards
- Report concerns about inappropriate content immediately
- Understand that AI systems may generate false, offensive, or harmful content
- Remain fully responsible for the legality, appropriateness, and safety of any AI-assisted output they use.

11. INCIDENT RESPONSE & REPORTING

All cyber incidents (including suspected breaches, malware, lost/stolen devices, phishing attacks, or denial of service) must be reported immediately to the IT Helpdesk. An incident log will be maintained.

Serious incidents will be escalated to:

- Headteacher & Governing Body
- Information Commissioner's Office (ICO) (within 72 hours if a data breach occurs).
- Police / Action Fraud (if criminal activity is suspected).

12. POLICY ENFORCEMENT

Cyber security incidents caused due to breaches of this policy by staff may result in disciplinary action as follows:

- First-time, unintentional, small-scale incident: We may issue a verbal or written warning, and provide additional training.
- Intentional, repeated or large scale incidents (which cause severe financial or other damage): We will invoke more severe disciplinary action up to and including termination.
- In addition, staff who are observed to disregard this policy will face progressive discipline, even if their behaviour hasn't resulted in a security incident
- We will examine each incident on a case-by-case basis.