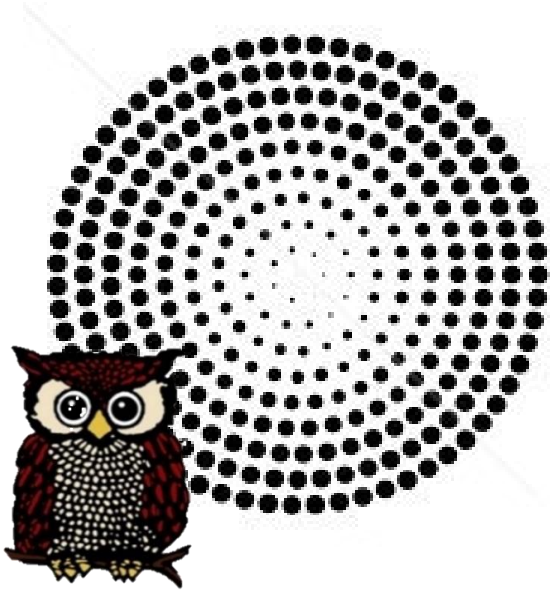
LGfL CyberCloud®

Cybersecurity Policy



Barham Primary School

Embedding Excellence

Cyber Security Policy

April 2026

Cybersecurity Policy

Cyber Security Policy 2025 - 2026

Barham Primary School

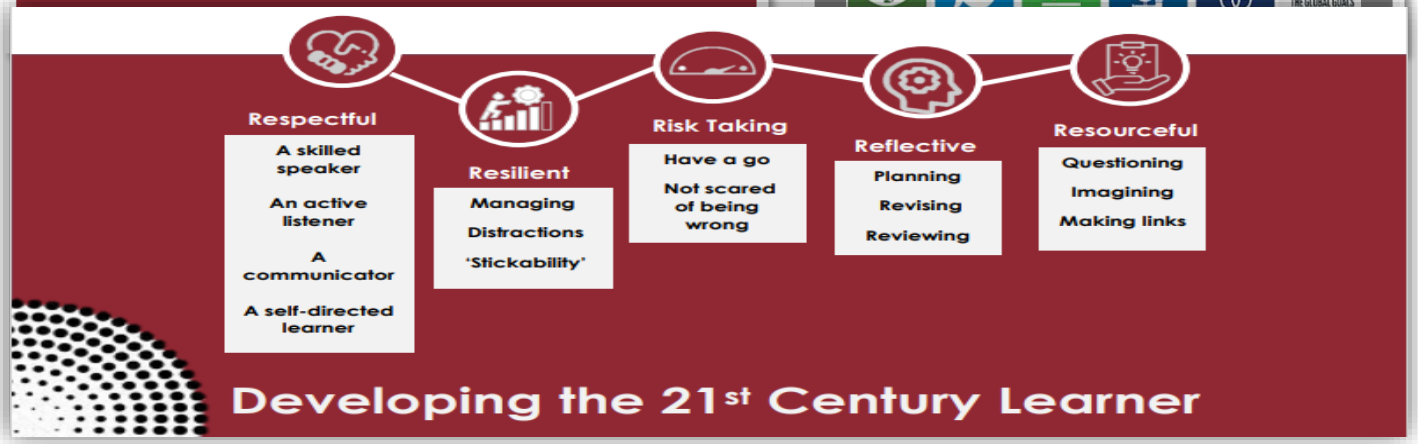
Embedding Excellence

What we want for our children

We want all of our children to leave us equipped for life in the 21st Century- able to operate successfully in the changing world of work and take advantage of all opportunities available to them. Through understanding our global community and appreciating our children's needs, we integrate specific learning experiences into our curriculum so that every child can achieve well at Barham, transition well into their next phase of education and lead happy and fulfilled lives.

Our vision

We are safe, happy and kind learners
We are ambitious and strive to reach the highest goals
We are curious and use connections to make sense of the world
We are change makers



Our vision and our values underpin all our policies; the education we deliver and are core to all our work. Article 3 of the United Nations Convention on the Rights of the Child states that: **The best interests of the child must be a top priority in all decisions that affect children. This policy has been created with this in mind to keep the children at Barham safe, happy, kind with a love for learning.**

Statutory Policy		
Last review	**Reviewed**	**Next Review**
April 2026	Annually	April 2027

LGfL CyberCloud®

Cybersecurity Policy

Introduction

A cybersecurity incident can have a major impact on any organisation for extended periods of time. For a school, this can range from minor reputational damage and the cost of restoring systems from existing backups, to major incidents such as losing student work or access to learning platforms and safeguarding systems, which could lead to data-protection fines or even failing an inspection.

This Cybersecurity Policy outlines **Barham Primary School's** guidelines and security provisions which are there to protect our systems, services and data in the event of a cyberattack.

Scope of Policy

This policy applies to all **Barham Primary School's** staff, contractors, volunteers and anyone else granted permanent or temporary access to our systems and hardware. It also covers the physical and technical elements that are used to deliver IT services for the school.

Risk Management

Barham Primary School's will include cybersecurity risks on an organisation risk register.

Physical Security

Barham Primary School will ensure there is appropriate physical security and environmental controls protecting access to its IT Systems, including but not limited to air conditioning, lockable cabinets, and secure server/communications rooms.

Cybersecurity Policy

Asset Management

To ensure that security controls to protect the data and systems are applied effectively **Barham Primary School's** will maintain asset registers for, files/systems that hold confidential data, and all physical devices (servers, switches, desktops, laptops etc) that make up its IT services.

User Accounts

Users are responsible for the security of their own accounts. If at any time they believe their credentials may have been compromised, for example after a phishing scam, they must inform the Network Manager as soon as possible, who will report the incident to senior leadership, arrange for new logins, passwords or suspend the account if necessary. Personal accounts should not be used for work purposes. Barham Primary School will implement multi-factor authentication where it is practicable to do so.

Devices

To ensure the security of all **Barham Primary School's** issued devices and data, users are required to:

- Lock devices that are left unattended
- Update devices when prompted
- Report lost or stolen equipment as soon as possible to **the Network Manager**
- Change all account passwords at once when a device is lost or stolen (and report immediately to **the Network Manager**
- Report a suspected threat or security weakness in Barham Primary systems to **the Network Manager**

Devices will be configured with the following security controls as a minimum:

- Password protection
- Full disk encryption where necessary
- Client firewalls
- Anti-virus / malware software such as Sophos and Malwarebytes
- Automatic security updates
- Removal of unrequired and unsupported software
- Autorun disabled
- Minimal administrative accounts

Data Security

Barham Primary School will take appropriate measures to reduce the likelihood of the loss of availability to, or the disclosure of, confidential data.

Barham Primary School's defines confidential data as:

- Personally identifiable information as defined by the ICO
- Special Category personal data as defined by the ICO
- Unpublished financial information

- Medical records, including GP names and medical conditions.
- Exam results and class grades.
- Staff development reviews.
- Safeguarding information, including data related to SEN assessments.

Critical data and systems will be backed up on a regular basis following methodology

- 2 versions of data
- 2 different types of media
- 1 copy offsite/offline

Sharing Files

Barham Primary School recognises the security risks associated with sending and receiving confidential data. To minimise the chances of a data breach users are required to:

- Consider if an email could be a phishing email or that a colleague's account could be 'hacked'. If something does not feel right check with the sender by another method, particularly in relation to financial transactions, attachments, or links to websites
- Wherever possible, keeping **Barham Primary School's** files on school systems
- Not sending school files to personal accounts
- Verifying the recipient of data prior to sending
- Using file encryption where possible, sending passwords/keys via alternative communication channels
- Alerting the **Network Manager** and or **Data Protection Officer** to any breaches, malicious activity or suspected scams

Training

Barham Primary School recognises that it is not possible to maintain a high level of Cybersecurity without appropriate staff training. **Barham Primary School** will provide annual Cybersecurity training for staff and arrange further training as necessary.

System Security

The Network Manger will build security principles into the design of IT services **Barham Primary School.**

- Security patching – network hardware, operating systems and software
- Pro-actively plan for the replacement of network hardware, operating systems and software before vendors stop providing security support for them
- Actively manage anti-virus systems
- Actively manage and test backups
- Regularly review and update security controls that are available with existing systems
- Segregate wireless networks used for visitors' & staff personal devices from school systems
- Review the security risk of new systems or projects

Cybersecurity Policy

Major Incident Response Plan

Barham Primary School will develop and maintain a Cybersecurity Major Incident Response Plan. This will include identifying or carrying out:

- Key decision-makers
- Key system impact assessments and restoration priorities (i.e. which backup needs to be restored first for the school to become operational again)
- Emergency plans for the school to function without access to systems or data
- Alternative methods of communication, including copies of contact details
- Emergency budgets and who can access them / how
- Key agencies for support (e.g. Remote IT Support and Data Backup Providers)

Maintaining Security

Barham Primary School understands that the financial cost of recovering from a Major Cybersecurity Incident can far outweigh the ongoing investment in maintaining secure IT systems. Barham Primary School will budget appropriately to keep cyber related risk to a minimum.

	Executive Headteacher	Georgina Nutton
	Head of School	Jayshree Thakore
	Chair of Governors	Daksha Thanki
	Network manager / other technical support	Paulette Williamson
	Date this policy was reviewed and by whom	April 2026 – Network Manager
	Date of next review and by whom	April 2027 – Network Manager