



**St. Stephen's Primary School**  
**Cyber Security**

<b>DATE APPROVED BY ST. STEPHEN'S CE PRIMARY SCHOOL</b>	Autumn Term 2024
<b>REVIEW DATE</b>	Autumn Term 2025
<b>APPROVED BY</b>	Full Governing Body

## 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 St. Stephen's CE School 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 St. Stephen's CE School 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

St. Stephen's CE School will include cybersecurity risks on its organisational risk register, regularly reporting on the progress and management of these risks to Governors termly. LGfL provide a Risk Register Template which is available [here](#)

### Physical Security

## Cybersecurity Policy

St. Stephen's CE 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.

### Asset Management

To ensure that security controls to protect the data and systems are applied effectively, St. Stephen's CE School 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 change their password and inform Click on it (CITL) as soon as possible. Personal accounts should not be used for work purposes. St. Stephen's CE School will implement multi-factor authentication where it is practicable to do so.

### Devices

To ensure the security of all St. Stephen's CE School 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 Click on it (CITL)
- Change all account passwords at once when a device is lost or stolen (and report immediately to Click on it (CITL)
- Report a suspected threat or security weakness in St. Stephen's CE School's systems to the school business leader.

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

- Password protection
- Full disk encryption
- Client firewalls
- Anti-virus / malware software eg Sophos and Malwarebytes for LGfL schools – see [sophos.lgfl.net](https://sophos.lgfl.net) / [malwarebytes.lgfl.net](https://malwarebytes.lgfl.net)
- Automatic security updates

## Cybersecurity Policy

- Removal of unrequired and unsupported software
- Autorun disabled
- Minimal administrative accounts

### Data Security

St. Stephen's School will take appropriate measures to reduce the likelihood of the loss of availability to, or the disclosure of, confidential data.

St. Stephen's 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

Critical data and systems will be backed up on a regular basis following the 3-2-1 backup methodology

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

[LGfL provide Gridstore as an online backup – see [gridstore.lgfl.net](http://gridstore.lgfl.net) ]

### Sharing Files

St. Stephen's 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 St. Stephen's 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 [IT Support/DPO] to any breaches, malicious activity or suspected scams

### Training

## Cybersecurity Policy

St. Stephen's School recognises that it is not possible to maintain a high level of Cybersecurity without appropriate staff training. It will integrate regular Cybersecurity training into Inset days, provide more specialist training to staff responsible for maintaining IT systems and promote a "No Blame" culture towards individuals who may fall victim to sophisticated scams. All school staff complete Cyber security Training for School Staff provided by the National Cyber Security Centre.

LGfL offer [Cyber Security Training for School Staff](#) and [Sophos Phish](#), a phishing simulation tool that links to training material

### System Security

Click On It (CITL) will build security principles into the design of IT services for St. Stephen's 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

### Major Incident Response Plan


St. Stephen's School will develop, maintain, and regularly test 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 backups 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. IT support company)

## Cybersecurity Policy

### Maintaining Security

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

	Headteacher / Principal	Elizabeth Bachour
	Chair of Governors	Alice Bishop
	Network manager / other technical support	LGFL CITL (Click on It)
	Date this policy was reviewed and by whom	06/09/2024 Crystal Taylor, School Business Leader
	Date of next review and by whom	Autumn 2025 Crystal Taylor, School Business Leader