The Federation of Sacred Heart and St Mary's RC Primary Schools, Battersea

CYBER SECURITY POLICY

Approved By	Governors
Reviewed On	September 2023
Review Due	September 2024
Review Cycle	Annually

Contents

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 Sacred Heart and St Mary's RC Primary School's guidelines and security provisions which are there to protect our systems, services and data in the event of a cyberattack. Wandsworth IT are our LA IT support service who we work closely with to maintain and protect our infrastructure.

Scope of Policy

This policy applies to all Sacred Heart and St Mary's RC 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

Sacred Heart and St Mary's RC Primary Schools will include cybersecurity risks on its organisational risk register, regularly reporting on the progress and management of these risks to Governors 3 times a year in the resources committee meetings.
[LGfL provide a Risk Register Template which is available here]

Physical Security

Sacred Heart and St Mary's RC Primary Schools 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, Sacred Heart and St Mary's RC Primary Schools will maintain asset registers for, files/systems that hold confidential data, and all physical devices (services, switches, desktops, laptops etc.) that make up its IT services. Wandsworth IT, our IT support Service also can view our connected assets via their asset management tool, 'Centrastage'

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 Wandsworth IT as soon as possible. Personal accounts should not be used for work purposes. Sacred Heart and St Mary's RC Primary Schools will implement multi-factor authentication where it is practicable to do so.

Devices

To ensure the security of all Sacred Heart and St Mary's RC Primary Schools 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 Wandsworth IT
- Change all account passwords at once when a device is lost or stolen (and report immediately to Wandsworth IT
- Report a suspected threat or security weakness in Sacred Heart and St Mary's RC Primary School's systems to Wandsworth IT.

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

- Password Protection
- The Device Build / Setup does not include full disk encryption for any devices as no data is taken off site. RDS (Remote Desktop Server) has been installed for staff working from home who need access to school's data.
- All schools are setup with the latest version of Sophos End point security from the LGfL (server and clients) as standard which we manage via the Sophos console on the server. Malware bytes (via LGfL) is another product available to us for use with schools but as yet is not an enterprise level solution with a management console – Wandsworth ICT support deploy Malware bytes on a case-by-case basis where needed.
- Removal of unrequired and unsupported software that we notify Wandsworth IT of.
- Minimal administrative accounts.

Data Security

Sacred Heart and St Mary's RC Primary Schools will take appropriate measures to reduce the likelihood of the loss of availability to, or the disclosure of, confidential data.

Sacred Heart and St Mary's RC Primary Schools 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

Sacred Heart and St Mary's RC Primary schools are currently using LGFL Gridstore for off-site backups of critical school's data (SIMS and core admin user data).

[LGfL provide Gridstore as an online backup – see gridstore.lgfl.net]

Sharing Files

Sacred Heart and St Mary's RC Primary Schools 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 Sacred Heart and St Mary's RC 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 [IT Support/DPO] to any breaches, malicious activity or suspected scams.

Training

Sacred Heart and St Mary's RC Primary Schools 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. [LGfL offer Cyber Security Training for School Staff and Sophos Phish, a phishing simulation tool that links to training material] Wandsworth City Learning Centre can support with this.

System Security

Wandsworth IT will build security principles into the design of IT services for Sacred Heart and St Mary's RC Primary Schools:

- Security patching – operating systems, network attached storage 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

Sacred Heart and St Mary's RC Primary Schools 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).

Maintaining Security

Sacred Heart and St Mary’s RC Primary Schools understands that the financial cost of recovering from a Major Cybersecurity Incident can far outweigh the ongoing investment in maintaining secure IT systems. Sacred Heart and St Mary’s RC Primary Schools will budget appropriately to keep cyber related risk to a minimum.

The Federation of Sacred Heart and St Mary’s RC Primary School, Battersea	Headteacher / Principal	Jared Brading
	Chair of Governors	Andrew Cooper Annabel Clarkson John O’ Brien Matthew Somorjay
	Network manager / other technical support	Wandsworth IT