



POLICY · STATUTORY & LEGAL

Cybersecurity Policy

Reviewed 2025–2026

ABOUT THIS POLICY

How we protect school systems, staff devices and pupil data from cyber threats. Aligned with the DfE's cyber-security standards for schools.

The full policy follows from the next page.

We want every child to be curious, have big dreams and be prepared for an exciting future.

01273 453176 · office@sgprimary.co.uk

Headteacher: Mrs Naomi Doble · Swiss Gardens Primary School, a maintained school in West Sussex

Swiss Gardens Primary School

Cyber Security Policy 2025/26



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 Swiss Gardens 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 Swiss Gardens staff, contractors, volunteers and anyone else granted permanent or temporary access to our systems and hardware.

Named Computing and E-safety co-ordinators

Naomi Welsh (Headteacher)

Claire Older (Assistant Headteacher – Safeguarding Lead)

Michelle Treasure (School Business Manager)

Gordon Oakley (Entrust Support Services – Infrastructure Technician)

Jasmyn La Coste (Subject Leader, Computing)

What is Cyber Crime?

Cyber-crime is simply a criminal activity carried out using computers or the internet. hacking, phishing, malware, viruses or ransom attacks. The following are all potential consequences of cyber-crime which could affect an individual and/or individuals:

- cost
- confidentiality and data protection
- potential for regulatory breach
- reputational damage
- business interruption
- structural and financial instability.

Data and Information Used

- Student and Staff information in our Management Information System (BROMCOM)
- Child Protection information (CPOMS)
- Communication – emails and messages through office 365 (Outlook)
- Curriculum and Teaching materials
- Records of information (meetings, presentations, etc)

Cyber Crime Prevention

Given the seriousness of the consequences noted above, it is important for Swiss Gardens to take preventative measures and for staff to follow the guidance within this policy.

Swiss Gardens have implemented the following technical measures to protect against cyber-crime:

- firewalls
- anti-virus software
- anti-spam software
- auto or real-time updates on our systems and applications
- URL filtering
- secure data backup
- encryption
- deleting or disabling unused/unnecessary user accounts
- deleting or disabling unused/unnecessary software
- using strong passwords
- disabling auto-run features

Asset Management

To ensure that security controls to protect the data and systems are applied effectively, Swiss Gardens 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 Entrust/Michelle Treasure as soon as possible.

In general, staff should try to only use school-issued devices to access school emails, accounts or folders. We advise our staff to keep both their personal and school-issued computer secure.

They can do this if they:

- Keep all devices password protected.
- Ensure that the school-installed antivirus software is installed on their school owned computer and that they have anti-virus software installed on home computers/devices.
- Ensure they do not leave their devices exposed or unattended.
- Ensure that school-wide security updates of browsers and systems have taken place.
- Log into school accounts and systems through secure and private networks only.

Devices

To ensure the security of all Swiss Gardens 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 Entrust
- Change all account passwords at once when a device is lost or stolen (and report immediately to Entrust)
- Report a suspected threat or security weakness in Swiss Garden's systems to Entrust/Michelle Treasure

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

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

Data Security

Swiss Gardens will take appropriate measures to reduce the likelihood of the loss of availability to, or the disclosure of, confidential data.

Swiss Garden'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

Sharing Files

Swiss Gardens 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 Swiss Garden'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] to any breaches, malicious activity or suspected scams

Keep Emails Safe

Emails often host scams and malicious software (e.g. worms.) To avoid virus infection or data theft, we instruct staff to:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. "watch this video, it's amazing.")
- Be suspicious of clickbait titles (e.g. offering prizes, advice.)
- Check email and names of people they received a message from to ensure they are legitimate.
- Look for inconsistencies or give-aways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)
- If a member of staff isn't sure that an email they received is safe, they can refer to Entrust or Michele Treasure.

See the section in the Acceptable Use of ICT Policy for further details on email etiquette and email security.

System Security

Entrust will build security principles into the design of IT services for Swiss Gardens

- 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

Manage Passwords Properly

Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they won't be easily hacked, but they should also remain secret. For this reason, we advise our staff to:

- 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). General guidance on creating a password is to take three random words and to add a number and a special character – eg. DinosaurStarRose14%
- Remember passwords instead of writing them down. If staff need to write their passwords, please keep passwords and identifiers separate or, at least, secure.
- Exchange credentials only when absolutely necessary. When exchanging them in person isn't possible, staff should prefer the phone instead of email, and only if they personally recognize the person they are talking to.
- Whilst some providers and organisations with whom we work advise (and expect) passwords to be changed regularly, we advise that passwords only be changed if and when they are compromised.

Cyber Crime Incident Management Plan

The incident management plan consists of four main stages:

- (i) Containment and recovery: To include investigating the breach, utilising appropriate staff to mitigate damage and where possible, to recover any data lost.
- (ii) Assessment of the ongoing risk: To include confirming what happened, what data has been affected and whether the relevant data was protected. The nature and sensitivity of the data should also be confirmed, and any consequences of the breach/attack identified.
- (iii) Notification: To consider whether the cyber-attack needs to be reported to regulators (for example, the ICO and National Crime Agency) and/or colleagues/parents as appropriate.
- (iv) Evaluation and response: To evaluate future threats to data security and to consider any improvements that can be made.

Maintaining Security

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

Swiss Gardens Primary School 	Headteacher / Principal	Naomi Welsh
	Chair of Governors	Sue Uff
	Network manager / other technical support	Michelle Treasure/Entrust
	Date this policy was reviewed and by whom	October 2025 Jasmyn La Coste
	Date of next review and by whom	October 2026 Jasmyn La Coste