Rosh Pinah Primary School

Cyber Security Policy

Updated: September 2025
Date for Review: September 2026

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 Rosh Pinah 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 Rosh Pinah 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

Rosh Pinah Primary School will include cybersecurity risks on its organisational risk register, regularly reporting on the progress and management of these risks to the Finance & Operation Committee 3 times a year.

Physical Security

Rosh Pinah 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.

Asset Management

Rosh Pinah Primary School will ensure that security control protects the data and effective systems are applied. The 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 the Headteacher as soon as possible. Personal accounts should not be used for work purposes. Rosh Pinah Primary School will implement multi-factor authentication where it is practicable to do so.

Devices

To ensure the security of all 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 the School Office
- Change all account passwords at once when a device is lost or stolen (and report immediately to the Headteacher
- Report a suspected threat or security weakness in School's systems to the Headteacher

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

- Password protection
- Client firewalls
- Anti-virus / malware software e.g. Sophos and Malwarebytes for LGfL schools
- Automatic security updates
- Removal of unrequired and unsupported software
- Autorun disabled
- Minimal administrative accounts.

Data security

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

Rosh Pinah Primary School 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 By the IT Technician.

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

Sharing Files

Rosh Pinah Primary School recognises the security risks associated with sending and receiving confidential data. To minimise the chances of a date 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 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

Rosh Pinah Primary 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 (LGfL offer Cyber Security Training for School Staff and Sophos Phish, a phishing simulation tool that links to training material).

System Security

'ICT Consultancy Services Limited' manages the whole IT network systems at Rosh Pinah Primary School:

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

Disaster Recovery Plan

- A full back up of the server is taken every night onto a separate fireproof / waterproof back up unit. This allows users to revert to previous versions of their files
- The Admin data is additionally backed up offsite by LGFL daily
- Staff passwords for the school server are kept securely on the server. The LGFL passwords are kept separate on the LGFL platform. The nominated contact for both systems is ICTCS Manager and Technician
- All new hardware is purchased with manufacturers warranty. Working parts are taken from obsolete machines to repair those outside of warranty and items that cannot be repaired are disposed of according to the WEE guidelines
- Appropriate technical and organisational measures are in place to safeguard personal information
- Methods of handling personal information are regularly assessed and evaluated. Records of personal information will not be kept for longer than is necessary and will follow the guidance in the Data Retention Policy and advice from Judicium.

Maintaining Security

Rosh Pinah 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. Rosh Pinah Primary School will budget appropriately to keep cyber related risk to a minimum.