NEW HEIGHTS SCHOOL
Focus · Learn · Achieve

Information Security Policy

Status	**Non-Statutory**
Responsible Governors' Committee	**Full Governing Body**
Date last approved by GB	**November 2025**
Responsible Person	**Co-Headteachers**
Review Date	**November 2026**
Last Amended Date	**November 2024**

SUMMARY

The objectives of the Policy, which is intended for all school staff, including Governors, who use or support the school's ICT systems or data, are to:

- Ensure the protection of confidentiality, integrity and availability of school information and assets.
- Ensure all users are aware of and fully comply with all relevant legislation.
- Ensure all staff understand the need for information and ICT security and their own responsibilities in this respect.

The integrity of New Heights School's network depends on the security policy being implemented and followed by its staff.

Information covers any information, including electronic capture and storage, manual paper records, video and audio recordings and any images, however created.

The school's System Manager is responsible for the school's ICT equipment, systems and data with direct control over these assets and their use, including responsibility for access control and protection. The System Manager will be the official point of contact for ICT or information security issues.

At New Heights School, this responsibility falls to Liverpool City Council and its sub-contractor, MICT.

Responsibilities:

- Users of the school's ICT systems and data must comply with the requirements of the ICT Security Policy
- Users are responsible for notifying the Headteacher or Deputy of any suspected or actual breach of ICT security. In their absence, users should report any such breach directly to the Headteacher. In the event of both being absent, the School Administration needs to be advised so SLT can be informed.
- Users must comply with the requirements of the Data Protection Act 2018, Computer Misuse Act 1990, Copyright, Designs and Patents Act 1988 and the Telecommunications Act 1984.
- Users must be provided with suitable training and documentation, together with adequate information on policies, procedures and facilities to help safeguard systems and data.
- Adequate procedures must be established in respect of the ICT security implications of personnel changes.

Physical Security:

- As far as practicable, only authorised persons should be admitted to rooms that contain servers or provide access to data. (At New Heights: Deputy Head, Operations Director, ICT co-ordinator and ICT technician)
- Server rooms must be kept locked when unattended.
- Appropriate arrangements must be applied for the removal of any ICT equipment from its normal location. These arrangements should take into consideration the risks associated with the removal and the impact these risks might have.
- All school owned ICT equipment and software should be recorded and an inventory maintained.
- Uninterruptible Power Supply (UPS) units are recommended for servers and network cabinets.
- Computer monitors should be positioned in such a way that information stored or being processed cannot be viewed by unauthorised persons.
- Equipment should be sited to avoid environmental damage.

- Do not leave sensitive or personal data on printers, computer monitors or desk whilst away from your desk or computer.
- Do not give out sensitive information unless the recipient is authorised to receive it.
- Use the school's secure email system to send sensitive / personal information
- Ensure sensitive data, both paper and electronic, is disposed of properly, e.g. shred paper copies and destroy disks.
- Ensure that notebooks / laptops are put away securely at the end of the day.

System Security:

- Users must not make, distribute or use unlicensed software or data.
- Users must not make or send threatening, offensive or harassing messages.
- Users must not create, possess or distribute obscene material.
- Users must ensure they have authorisation for private use of the centre's computer facilities.
- The System Manager will determine the level of password control.
- Passwords should be memorised. If passwords must be written down they should be kept in a secure location.
- Passwords should not be revealed to unauthorised persons.
- Passwords should not be obvious or guessable and their complexity should reflect the value and sensitivity of the systems and data.
- Passwords should be changed at least termly.
- Passwords must be changed if it is affected by a suspected or actual breach of security, e.g. when a password may be known by an unauthorised person.
- Regular backups of data, in accordance with the recommended backup strategy, must be maintained.
- Security copies should be regularly tested to ensure they enable data restoration in the event of system failure.
- Security copies should be clearly marked and stored in a fireproof location and/or off site.

Virus Protection:

- The System Manager will ensure current and up to date anti-virus software is applied to all centre ICT systems.
- Laptop users must ensure they update their virus protection at least weekly.
- The System Manager will ensure operating systems are updated with critical security patches as soon as these are available.
- The System manager will ensure users of home/centre laptops check for critical security patches/Anti-virus updates when connecting laptops to the centre network.
- Any suspected or actual virus infection must be reported immediately to the System Manager.

Disposal and Repair of Equipment:

- The System Manager must ensure any personal data or software is obliterated from a PC if the recipient organisation is not authorised to receive the data.
- It is important to ensure that any software remaining on a PC being relinquished are legitimate. Care should be taken to avoid infringing software and data copyright and licensing restrictions by supplying unlicensed copies of software inadvertently.
- The System Manager must ensure the requirements of the Waste from Electronic and Electrical Equipment (WEEE) Directive are observed.
- The school will ensure that third parties are registered under the Data Protection Act as personnel authorised to see data and as such are bound by the same rules as school staff in relation to not divulging the data or making any unauthorised use of it.

Security Incidents:

All suspected or actual breaches of the ICT security, including detection of computer viruses, must be reported to the Co-Headteachers immediately. In their absence, report it to the Operations Director.