All Saints
Infants School

Information and ICT Security Policy

Learning with love and Laughter

Policy written by:	Headteacher
Approved by Headteacher on:	April 2025
Approved by Governors on:	April 2025
Date of next review:	April 2028
Policy owner:	Headteacher
Location of policy School:	Website/intranet
Policy control record updated by Clerk to Governors:	Yes
Date of last amendments:	January 2022

Schools' Information and ICT Security Policy

The purpose of Internet access in school is to enhance teaching and learning and to enhance the school's management information and business administration systems. Access to the Internet is a necessary tool for all staff and a privilege for students irrespective of gender, race, religion, culture, or ability. 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 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.

Information covers any information, including electronic capture and storage, manual paper records, video and audio recordings and any images, however created. The school ICT lead (Stewart Thomas) 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. An employee of the school, the ICT Lead will be the official point of contact for ICT or information security issues.

RESPONSIBILITIES

- Users of the school's ICT systems and data must comply with the requirements of the Information and ICT Security Policy.
- Users are responsible for notifying the ICT Lead of any suspected or actual breach of ICT security. In exceptional circumstances, users may report any such breach directly to the Headteacher, Chair of Governors or to Internal Audit.
- Users must comply with the requirements of the Data Protection Act 2018, Computer Misuse Act 1990 and Copyright, Designs and Patents Act 1988.
- 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 have access to computers that contain servers or provide access to data.
- 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 should be recorded and security-marked, subject to return conditions for leased equipment.
- An inventory of school hardware and software must be 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 person is authorized to receive it.
- Do not send sensitive/personal information via e-mail or post without suitable security measures being applied.
- Ensure sensitive data, both paper and electronic, is disposed of properly, e.g. shred paper copies and destroy disks.

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 school's computer facilities.
- The ICT Lead will determine the level of password control.
- Passwords should be memorised.
- 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 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 case of system failure.
- Where possible, security copies should be clearly marked and stored in a fireproof location and/or off site.

VIRUS PROTECTION

- The ICT Lead will ensure current and up to date anti-virus (AV) software is applied to all school ICT systems.
- The ICT Lead will ensure operating systems are updated with critical security patches as soon as these are available.
- The ICT Lead will ensure users of home/school laptops check for critical security patches/AV updates when connecting laptops to the school network.
- Any suspected or actual virus infection must be reported immediately to the ICT Lead.

DISPOSAL AND REPAIR OF EQUIPMENT

- The School Information Security Officer 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 ICT Lead 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.

Reviewed: April 2025
Approved: April 2025
Next Review: April 2028