Ashleigh

Primary School

ICT Security

Policy

Written by: IM – February 2022

Reviewed Sept 2025

Staff: Sept 2025

Approved by Governors: Sept 2025

Review date: Sept 2027

**Objectives of the Policy**

The purpose of this policy is to protect the School’s information asset by ensuring the:

Availability: information is and continues to be accessible and usable as normally required

Integrity: information is assured with regard to version, accuracy, and freedom from corruption

Confidentiality: information is restricted to the people and for the purposes intended

The primary aim of this policy is to protect our school community and its data from security threats. It provides a framework for the acceptable and secure use of all school ICT systems, including personal devices.

**Definition and Classification of Information**

Information within this Policy means data, programs, documents, spreadsheets, databases, electronic mail messages, images and maps of all types regardless of how or where within the School the information is stored or managed.

**Information Backup**

The headteacher/SLT must make sure that appropriate procedures are in place to maintain the confidentiality of the information and to recover from the temporary or permanent loss of the information or supporting equipment.

All information must be protected by a procedure for archiving and copying for security backup. The procedure must incorporate daily, weekly, monthly, year end cycles appropriate to the type of information, frequency of update, legal and operational requirements.

Security back up copies to be stored wherever possible away from the location at which the operational information is maintained.

The ability to restore information from back-up copies must be tested periodically to ensure that procedures, equipment and storage media are performing correctly.

**Compliance With Legal Requirements**

All computer media must be stored and disposed of with due regard to its sensitivity and the requirements of the Data Protection Act.

Disclosure of information must be in accordance with the Data Protection Act.

**General Compliance**

Unlicensed, illegal or unauthorised software or information must not be installed, used, copied, altered or distributed.

Illegal or improper access to external networks, services or facilities is prohibited.

**Access Control**

In accordance with section 5 of the Financial Regulations the Director of Finance and IT’s auditors will have access as necessary to any information and applications systems.

Any method of log-on which nullifies the password control is prohibited

Passwords must not be printed or displayed on input

Each user must have their own user ID and password. The use of another person’s user-ID is not allowed.

Passwords must be a minimum of five characters and must be changed in accordance with procedure and immediately it is suspected that the password has been disclosed.

The change should be to a previously unused password.

Access rights for all leavers should be removed immediately.

Access rights for all users should be reviewed and updated periodically.

**Equipment**

The Headteachers is responsible for IT facilities installed within the school and for ensuring their proper use. The use of IT facilities not directly concerned with the School’s business is prohibited.

All items of equipment must be security marked in accordance with the School’s risk management policy and included on the inventory.

Wherever equipment is kept in an area that is unsecure, accessed by members of the public or unsupervised representatives of other organisations, the following measures are in place for additional protection;

* Fire detection and prevention
* Intruder alarm
* CCTV

Where equipment is located within areas accessed by members of the public or in unsecured offices and left unattended for periods of time, the following measures have been considered to deter the theft of that equipment:

* Improved security of the outer walls and windows

Terminals and PC’s must not be left unattended when logged in to applications. If not in use they must be logged out or protected by a secure screen saver. Users must log out of the systems and the network before signing out of work and also switch off their terminal/PC/printer.

**Personal Systems and Portable PCs**

No equipment must be removed from its location without the permission of the Headteacher who must be satisfied that appropriate arrangements have been made for insurance of equipment and information.

The removal of this equipment should be recorded and monitored.

Equipment **must not be left in unattended vehicles** for which insurance is not available.

**Disposal of Obsolete Computer Equipment**

The disposal of obsolete computer equipment is governed by the Schools ‘Scheme of Financial Administration’.

The Governing Body should authorise all write offs and disposals of surplus stocks and equipment in accordance with LA or DCFS regulations.

All information has been physically deleted, corrupted or overwritten so as to make it irrecoverable.

Software is not offered to an external agency unless there is a legal right to do so and licence records are adjusted accordingly.

The inventory is updated to record the disposal.

This policy has been developed in line with current legislation, including the **UK General Data Protection Regulation (UK GDPR)**, the **Data Protection Act 2018**, and the principles of the Department for Education’s statutory guidance, **"Keeping Children Safe in Education."** Safeguarding is everyone's responsibility, and this duty applies to the online world as it does to the physical world.

**Roles and Responsibilities**

* **The Headteacher (Mr. I. Matthews):** Holds overall responsibility for the implementation of this policy and acts as the Designated Safeguarding Lead (DSL) for online safety concerns.
* **The Governing Body:** Is responsible for approving this policy and monitoring its effectiveness. The designated governor for Computing is Les Campbell, and the governor for Health, Safety & Safeguarding is also Les Campbell.
* **The Computing Lead (Mr. I. Thomson):** Is responsible for overseeing the technical implementation of this policy, managing security systems, and supporting staff.
* **All Staff:** Are responsible for reading, understanding, and adhering to this policy. All staff must complete annual training in Safeguarding, Child Protection, PREVENT, and Online Safety. They are expected to model safe and professional online behaviour at all times.
* **Pupils:** Are taught to use ICT safely and responsibly through the PSHE curriculum and are expected to follow the school's acceptable use rules.

**Data Protection and Security**

The school is committed to complying with the UK GDPR in its handling of all personal and sensitive data.

* **Confidentiality:** Staff are expected to treat all information they receive about children and families in a discreet and confidential manner. Sensitive data must not be stored on unencrypted personal devices or removable media.
* **Password Security:** All users must have a strong, unique password for school systems. Passwords must not be shared with anyone. Staff should lock their computers when leaving them unattended.
* **Network Security:** The school network is protected by appropriate firewalls, filtering, and monitoring systems. This is to prevent access to inappropriate or harmful content and to fulfil our PREVENT duty.
* **Device Security:** All school-owned devices are managed and monitored by the school. Any personal devices used for school purposes must be appropriately secure and used in line with this policy.

**4. Acceptable Use of Technology**

**4.1 Use of School Systems**

School ICT equipment and systems must be used professionally and responsibly. Staff must follow the school's policy on the use of IT equipment. Prohibited activities include:

* Accessing, downloading, or distributing any illegal, obscene, or offensive material.
* Publishing untrue or defamatory statements about the school, its staff, or pupils.
* Using school systems for personal financial gain or significant private use.

**4.2 Mobile Phone Usage**

The rules outlined in the Staff Handbook are a core part of this policy:

* Mobile phones must not be used for personal reasons during lessons or formal school time.
* Use of mobile phones for social networking during working hours is strictly prohibited.
* Staff are not permitted to use their own mobile phones to contact children or their families in a professional capacity, except in an emergency.
* Mobile phones are not permitted in designated areas such as changing rooms and toilets.

**4.3 Use of Images and Video**

Staff must be clear about the purpose of any photography or recording. Staff must not take, display, or distribute images of children unless they have consent to do so. All images must be stored securely on the school's network.

**Online Safety and Incident Reporting**

5.1 Online Safety

Our commitment to safeguarding underpins our approach to online safety.

* Filtering and Monitoring: To protect pupils from harmful and inappropriate online content, the school's network is filtered using the Surf Protect system. In addition, all school devices are actively monitored in real-time using the Securus system. This allows for the swift identification of any safeguarding concerns, enabling staff to provide immediate support to pupils.
* Cyberbullying: Online bullying and harassment will not be tolerated. Any staff member who feels they have been a victim should report it to the Headteacher. Concerns about pupils should be reported to the DSL.
* Training and Education: Staff receive annual online safety training, and pupils are taught how to stay safe online through the curriculum.

**5.2 Reporting Procedures**

* Technical Incidents: Any suspected security breaches, such as a virus, phishing attempt, or data loss, must be reported immediately to the Computing Lead (Mr. Thomson) or the Headteacher.
* Safeguarding Concerns: Any online safety concern, including cyberbullying, inappropriate contact, or exposure to harmful content, must be reported immediately to the DSL (Mr. Matthews) or Deputy DSL (Mr. Harty). All such concerns must be recorded on the school's system, CPOMS.

**6. Links to Other Policies**

This policy should be read in conjunction with the following school policies:

* Safeguarding and Child Protection Policy
* Staff Code of Conduct
* Behaviour Policy
* Anti-Bullying Policy
* Social Media Policy