Sandridge Primary School

ICT & Cyber Response Plan

The policy was reviewed and ratified by the Governing Body on 20th March 2025.

This policy will be reviewed, in full, every three years.

It is due for review in March 2028.

Introduction

ICT enables and enhances Sandridge School's educational and organisational vision and objectives. Information stored on school ICT devices and related systems must be protected to preserve confidentiality, integrity and availability in order to help enable the school's vision and aims to be achieved.

Purpose

The purpose of the ICT & Cyber Response Plan is to clarify responsibilities and security measures to be undertaken in accordance with regulatory, legislative and local requirements to ensure that information remains confidential, protected from unauthorised access or disclosure; accessible and available and that data integrity is not compromised. In the event of a cyber attack or data loss, please refer to the Data Protection Policy & Data Breach Response Plan (the cyber response team and actions are detailed within that policy).

Scope

This Plan is intended for school-owned ICT equipment and systems when held internally or outside the main office. It is intended for anyone who has access to the school's administrative and/or curriculum ICT systems or data.

For this Plan definitions are as follows:

- Information covers any method of information creation or collection, including electronic capture and storage, video and audio recordings and any images.
- ICT or ICT system means computing and communications facilities that support teaching, learning and a range of activities in education.
- ICT is the knowledge, skills and understanding needed to employ information and communication technology appropriately.
- ICT equipment means computers, laptops, Chromebooks, iPads, tablets, cameras and mobile phones.
- This Plan incorporates the best practice and follows guidance from the National Cyber Security Centre's '10 Steps to Cyber Security' in the safe and secure storage of electronic files and data (*see* ***Appendix A***).

Responsibility

The school Governing Body has ultimate responsibility for setting and enforcing this Plan. The Headteacher is responsible for ensuring that the requirements relating to this Plan are adopted and that the information and guidance set out within this policy is adhered to. The Headteacher, alongside the school Computing Lead have overall responsibility for the implementation of the ICT security arrangements within the school; it is their responsibility to ensure measures are implemented consistently and effectively and are free from discrimination.

The school's IT support team (Con-Ed) are responsible for ensuring that security measures are installed on ICT systems and regularly monitored for security compliance; advising of

any suspected or actual ICT security breaches and ensuring a Data Security document (a system overview) is in place.

Everyone who has access to the school's ICT systems and data must comply with this policy, in addition to complying with the Data Protection Policy & Data Breach Response Plan.

Anyone who has access to school data is required to read, accept and agree to follow these policies in order to protect personal data as outlined by the General Data Protection Regulation.

ICT asset accountability and control

Procurement

- Procurement of ICT equipment, services and software must be agreed with the Headteacher as an initial first step
- An ICT Asset Register will be maintained by Con-Ed. All items will be accounted for annually. In addition, a software and license register is kept updated.
- No software which will be used to process personal data should be used before a Data Protection Impact Assessment (where required by regulation) has been undertaken.

Repairs and Relocation

- Users are required to contact Con-Ed to report any faults or problems they experience, whether hardware or software related.
- Connection, disconnection or relocation of any fixed ICT equipment must be undertaken in consultation with Con-Ed.
- Damaged or faulty devices must not be used and should be returned or reported immediately to Con-Ed.

Disposal & Loss of ICT Equipment

- ICT equipment identified for disposal or reuse will be held in secure storage until redeployed or disposed of. Disposal information must be recorded and noted on the ICT Asset Register.
- ICT equipment can either be completely wiped clean of data by Con-Ed or externally by a Waste Electrical and Electronic Equipment (WEEE) accredited compliant recycling partner, which *must* provide certificates as evidence of the secure destruction of data.
- Any loss of devices must be immediately reported to Con-Ed, who will arrange instant disablement and security measures of the device when and where possible.

Staff Departure

- All staff who leave the school's employment must return school owned ICT equipment as part of the leaving process.

Physical and environmental security

- All servers, networks and communications equipment including associated cabling will be held stored securely where possible/required, or housed in appropriate cabinets.
- Access to ICT servers will be restricted to authorised persons by manually lockable methods.

Equipment security

Equipment Placement and Protection

- Computer screens, keyboards, printers or other similar devices must be positioned so that information stored or being processed cannot be viewed by unauthorised persons.
- ICT equipment must be positioned so it is not damaged by dust and heat.
- With the exception of portable and mobile devices provided specifically for homeworking, employees are not permitted to remove ICT equipment from the school's premises.
- Devices must be held securely on and off school's premises.
- All desktop, portable and mobile devices will have a basic input output system (BIOS) password.
- Time appropriate automatic screen locking procedures for will be implemented for required users in the instance of inactivity over a period of time. A user's password will be required to unlock the screen in this event.
- Staff must ensure that all desktop, portable and mobile devices are locked prior to leaving them unattended.

Power Supplies

Critical hardware such as servers and communications equipment will be protected from power supply failure through the use of uninterruptible power supplies (UPS) which offer battery-based backup power.

Clock Synchronisation

In order to ensure the accuracy of logging and/or monitoring information, the time clocks on the School's servers and required ICT devices should be synchronised to a Network Time Protocol (NTP) source.

Security of data

All teaching staff and some support staff are in possession of confidential, sensitive and personal data about children and parents/carers and have an explicit duty under law to guard this data and use it appropriately. School takes the security of information very seriously and recognises our duties under the new General Data Protection Regulations of 2018.

Anti virus

- Anti-virus software is installed onto school servers and managed on every school owned networked device.

- Client devices are configured to automatically check and install updates at regular intervals.
- Any school owned portable and mobile ICT devices connected to the Internet must be allowed to install automated virus definition and windows security patch updates.
- Non networked ICT equipment e.g. laptops are installed with a standalone copy of anti-virus software which automatically displays a warning message once the virus definition is out of date. Users are required to contact IT Support to arrange regular updates of anti-virus software. Laptops must be connected to the school network at least once every 90 days.
- Any information taken from the Internet will be scanned for viruses before it is received on a school's local area network.
- Network devices or software designed to capture and/or analyse network traffic must not be installed on school networks without appropriate authorisation from IT Support.
- External email messages entering a school network will be automatically checked for malware and suspicious content and quarantined if necessary.
- Where/when a virus is detected, this must be reported immediately to IT Support. In the event of any suspicious content or security breaches on devices, IT Support will re-image and wipe devices to ensure best practices are followed and to ensure impacted devices are 'clean'.
- Users who attempt to install, store or use illegal, unapproved or copied software will be subject to appropriate disciplinary action.
- IT Support will implement and utilise firewall protection to prevent illegal intrusion via the Internet.

Information back-up

Back-Ups are completed at regular intervals and following best industry practice of the 3-2-1 strategy, where at a minimum two copies are backed up on site and one off site.

Instructions for re-installing data or files from back-up are fully documented and tested at regular intervals to ensure that they enable the systems and files to be re-loaded in cases of system failure.
Data will not be stored on unencrypted portable and mobile devices as these are not included in the automatic back-up of network servers.

Copies of data stored on back-ups are deleted in accordance with Data Retention (detailed in the school's Privacy Notice).

Authorisation

Only persons authorised by the Headteacher are permitted to use the school's ICT systems. Users will be required to follow all school policies and procedures regarding its use.

User privilege management

- Each system will permit access to a user only on entry of a legitimate unique name (User ID) and password. Users must only use their own unique username (User ID) and password to access a school network and not use other staff members profiles.
- Users' permissions and groups will be set and managed by IT Support; all requests for additional access and permissions will be applied by IT Support in conjunction with approval from a user's line manager or the Headteacher.
- Only specific staff have administrative privileges on school systems.
- There may be restricted access in place e.g. to different parts of systems, or to view, view and update or view, update and delete. Adding or disabling user accounts and setting up/amending user profiles forms part of electronic access arrangements in order to protect data.
- Users will only be supplied with the level of access/least privilege required to perform their work duties.
- Users must not attempt to gain access beyond their given access privileges. If additional access is required, permission and approval must be requested and granted.
- In the event of third parties requiring access, they will be provided with accounts that solely provide access to the systems and/or data they are contracted to handle, in accordance with least privilege and need to know principles.
- Third Party accounts will be removed at the end of the contract or when no longer required.
- After entering their unique name (User ID) and password to enter a school ICT system, users may be reminded of their security responsibilities which they must agree to before continuing.
- School will review user profiles on a regular basis to ensure that current access levels are still appropriate, user groups are updated, and that staff are removed/deleted when no longer working within the school or if user's requirement change.
- Personal User IDs must not be shared between people/groups.
- Access to 'Confidential' and 'Restricted' information will be limited to authorised persons whose roles require it and following this policy.
- Users who have resigned or no longer contracted will have all access to IT and systems revoked and terminated. In the event of access being required after this period and in unique circumstances, permission must be given by the Headteacher.
- All ICT equipment on loan to staff must be returned on their final day of employment, unless otherwise agreed with the Headteacher.
- Users who have been dismissed or subject to disciplinary action or criminal charges which may compromise the security of information systems must have access to School ICT systems revoked at the earliest opportunity.

Passwords

For guidance on passwords and management, please see **Cyber Security** below**.**

Cryptographic controls

- All staff laptops must have fully encrypted hard drives
- Removable Disk Media, such as USB Drives, are not permitted to be used on site without express permission of the Headteacher.
- Where technology prevents the use of encryption (e.g. memory cards used in Digital Cameras) personal data must not be stored on these devices.
- Emails sent outside the school network (except for secure portals e.g. Local Authority/DfE), where possible, should be encrypted if personal data is being sent. The de-encryption key must not be sent via the same medium as the encrypted data.
- Encryption and RADIUS Authentication is applied to wireless networks throughout the school, encryption keys will be kept secure and remain the property of IT Support and must not be shared without permission obtained from the Headteacher.

Operation system patching

- Network security vulnerabilities, missing patches and updates will be monitored and managed by IT Support.
- When it is known that a vulnerability is being actively exploited a patch will be applied immediately and systems will be adjusted and secured accordingly as appropriate.
- Operating systems will be patched and kept updated with the latest releases that are issued.
- Where legacy devices, software, applications and operating systems are in use that are no longer patchable or able to update, therefore becoming a security risk, an upgrade plan for these must be established and in place ASAP.

Filtering

Access to the internet is filtered using an approved system through our internet service provider. The Designated Safeguarding Lead is responsible for checking the filtering records. Any breaches that occur as a result from filtering, must be reported to the Headteacher.

Email, internet and social media

Emails should not include personal information unless documents contained are password protected or encrypted. Personal information should not be shared online without personal consent of the data subject (or parent/carer for our pupils, as they are under 13 years of age). Defamatory or sensitive personal information should not be shared publicly or with groups of people/platforms/social media.

Remote working / access

Remote employees must follow the guidelines within this policy. Since they will be accessing school information and systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is

secure. We encourage all staff who work remotely to seek advice from IT Support to ensure they are following best practices.

- School data should NOT be stored on any portable or mobile ICT device not belonging to a school (including USB memory sticks, cards and hard disks).
- Home working is permitted where authorised by the Headteacher. The installation of any applications or software packages on school owned portable and mobile devices must only be carried out by IT Support unless permission is granted by the Headteacher.
- Access to a school's network and school ICT equipment is not permitted to be taken outside the United Kingdom without prior permission from the Headteacher.
- Remote access of the school's network is strictly prohibited unless this is carried out through a method shared by senior staff as safe and correct. The use of software such as TeamViewer, Anydesk, Logmein etc. are also strictly prohibited and not allowed to be installed onto devices.

ICT security incidents

The school has mechanisms in place to properly react and deal with ICT security incidents and violations, both intentional and unintentional. This Data Protection Policy & Cyber Response Plan is in place to follow in the event of such an occurrence taking place.

All ICT security weaknesses and incidents, whether suspected or actual, are to be reported ASAP to a senior member of staff and to IT Support directly. Users must not attempt to prove or exploit a suspected ICT security weakness. ICT security incidents can include but are not limited to virus attacks, suspicious emails, hardware and software faults, theft or suspected theft of any ICT resources, equipment or information, breach of security resulting in internal fraud or suspected fraud, non-compliance with statutory requirements regarding privacy of information.

ICT security awareness / training

ICT security awareness mechanisms are in place to ensure anyone who has access to a school's ICT equipment and data are aware of the importance of ICT security, and to properly react and deal with ICT security incidents and weaknesses. User awareness will be supported by regular updates.

- All staff are required to complete Cyber Security Training for School Staff through the National Cyber Security Centre.
- GDPR staff training is delivered by the external DPO.
- Internal GDPR training is provided internally to new starters as required.

Monitoring

- Users of school systems or school provided internet connectivity should be aware that the privacy of/in any message, files, data, document, facsimile, telephone conversation, web search/login, social media post, conversation or message, or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on school owned electronic information and communications systems may be subject to monitoring and review.

- The school reserves the right to monitor, intercept and review, without prior notification or authorisation from users.
- Usage of School's IT resources and communications systems activities will be monitored to ensure that school rules are being complied with and for the following purposes:
    - to monitor whether the use of school systems and/or the internet is legitimate and in accordance with school policies
    - to assist in the investigation of wrongful and reported misuse
    - to comply with any legal obligation
- Users consent to monitoring by acknowledgement of the School's Code of Conduct and the use of school resources and systems. The school may store copies of data or communications for a period after they are created and may delete such copies from time to time without notice. If necessary, information may be handed to the Police in connection with a criminal investigation.
- Security audit logging is activated on required ICT devices and servers have security audit logging switched on to automatically record events such as failed logon attempts. Critical application systems such as School MIS and Finance systems will display information and unsuccessful login attempts.
- All Windows servers event logs are checked during regular server maintenance routines.
- The performance of school servers is continually reviewed as part of a regular Server maintenance schedule by IT Support. This includes a review of, but not limited to, system event logs, ICT device/alert messages and disk space.
- CCTV systems monitor school's within the school 24 hours a day, this data is recorded and may be used as evidence of any alleged wrongdoing. Please see the school's **CCTV Policy** for more information and guidance regarding CCTV within schools.
- The school reserves the right for appropriately elected employees to use approved software tools to monitor school network, systems and emails in order to check compliance with this and other school policies. This will be authorised by the Headteacher.

Disciplinary action

Disciplinary action may be taken against any user suspected of being in breach of this policy, including an immediate ban from using the school's ICT facilities and equipment. Breaches of this policy may constitute gross misconduct and as such may lead to staff dismissal. For individuals not directly employed by the school, breaches of the Policy may result in withdrawal of facilities, rights and immediate access removal. For all other users, a breach of this policy may constitute a breach of the Code of Conduct and may lead to sanctions being applied and further actions taken if deemed necessary.

The Police will be informed where there is a possibility that a criminal offense has been committed.
If an employee is aggrieved or wishes to register or report a complaint, they must follow the School's Whistleblowing Policy and/or Staff Grievance Procedures.

CYBER SECURITY & RESPONSE

This section covers the school's approach to Cyber Security guidelines and provisions for preserving the security of our ICT, data and technology infrastructure. Threats including human error, hacker attacks and system malfunctions can cause catastrophic financial damage and can put at risk the school's reputation. For this reason, we have implemented the following security measures and have developed clear and concise instructions to help mitigate security risks.

In the event of a cyber attack or data loss, please refer to the **Data Protection Policy & Data Breach Response Plan.** The Cyber Response Team and actions are detailed within that policy.

SCOPE

Cyber Security is the responsibility of all school employees, contractors, volunteers and any individual associated who has permanent or temporary access to our systems and hardware.

ELEMENTS

Confidential data

Confidential data is information that allows public identification, which might cause harm to a respondent or establishment if released. Common examples are:

- personal information relating to staff, pupils, parents/carers, governors and partners
- financial information
- sensitive and contractual data

All members of the school community who have access to personal data are obliged and responsible to protect it. This policy will outline and give guidance to all persons with access, on how to avoid security breaches and the best security measures to follow in relation to this.

Protecting personnel and school

When school staff use their devices to access school emails or accounts, there is a security risk introduced to our data. We advise and recommend all school employees and students to keep both their personal and school devices secure at all times. This can be achieved by:

- Ensuring all devices are password protected
- Ensuring antivirus on your devices is kept up to date.
- Ensuring devices are kept safe, secure and never left unattended
- Ensuring devices are securely locked away when possible
- Installing all security updates when prompted or as soon as updates are available
- Contacting and reporting to IT Support any concerns or suspicious activity
- Log into accounts and systems through secure and private networks only

We advise all school employees and students to avoid accessing internal systems and accounts from other people's devices and the lending of their personal devices to others.

Emails

Emails are often open to phishing attacks, scams or malicious software. To avoid the risk of these types of potential virus infections or data thefts, we advise all school employees and users to carefully follow the below steps:

- Avoid opening emails and attachments from unknown senders
- Be cautious of emails threatening to block, remove or requesting information
- Avoid opening emails and attachments from suspicious looking email addresses, for instance ***"@office365hotmail346.com"***
- Avoid opening attachments and clicking on links where content is not adequately explained, for instance ***"Click Here Now!"***
- Be suspicious of clickbait titles, offering prizes
- Check email addresses and names of people carefully to ensure the sender is legitimate
- Look for general inconsistencies and obvious indications such as: grammatical mistakes, inconsistent capital letters, excessive number of exclamation marks.) If a user isn't sure that an email they have received is safe, they should contact IT Support.

Never attempt to open or deal with a suspicious email yourself, IT Support will resolve and provide guidance and advice. It is vital to remember, when it comes to Cyber Security, no question is ever regarded as trivial. It is always considered best practice to report any uncertainty over emails.

Password management

Password leaks are incredibly dangerous, a single incident of password exposure can compromise and bring down the entire school infrastructure. It is imperative that passwords are not only secure to prevent them from being easily hacked, but they should also remain confidential and never shared. We ensure that all school staff and users have and follow:

- Passwords with the following rules and combination: eight characters minimum, preferably four or more unrelated words joined together.
- Remember passwords instead of writing them down. In the instance that passwords need to be written, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.
- Never exchange or share passwords with anyone outside of the school. If requested by IT Support, this should be shared in person or over the phone if you recognise the voice, never over email.
- System administrator passwords are kept in a secure and protected location with permissions and rights only to those requiring access.
- Administrative passwords will be immediately changed when anyone who has access rights leaves the school's employment.

Transferring of data

The transfer of data involves a security risk. To reduce this, users must:

- Avoid transferring sensitive data (e.g., pupil information, employee records) to other devices or accounts unless absolutely necessary.
- Only ever share confidential data over the school network/system and ***never*** over public Wi-Fi or private connection.
- Ensure that the recipients of the data are properly authorised and/or organisations that have adequate security policies.
- Report scams, privacy breaches and hacking attempts. IT Support need to be made aware about scams, breaches and malware so they can better protect our

infrastructure. For this reason, we advise our users to report perceived attacks, suspicious emails or phishing attempts as soon as possible.
- In the event of the above, IT Support will investigate promptly, resolve the issue and send a school-wide alert if necessary.
- IT Support is responsible for advising users on how to handle and proceed with the above. We encourage our users to reach out with questions.

Additional measures
To reduce the likelihood of security breaches, we also instruct all school data users to:
- Turn off their screens and lock their devices when leaving their desks.
- Report stolen or damaged equipment as soon as possible to IT Support or a member of SLT.
- Change all account passwords immediately if a device is stolen.
- Report a perceived threat or possible security weakness in school systems.
- Refrain from downloading suspicious, unauthorised or illegal software on school equipment.
- Avoid accessing suspicious websites. We also expect our users to comply with our School IT policies

IT Support will:
- Manage and keep the school's Network and infrastructure secure
- Inform employees regularly about potential threats and security concerns.
- Investigate instances of security breaches, security concerns and reports thoroughly.

IMPORTANCE OF SECURITY

Everyone should feel that their data is safe. We understand the importance of proactively protecting our systems and data. We can all contribute to this by being vigilant and keeping cyber security in mind.

SAFEGUARDING

Schools have a statutory duty to monitor their digital environment to identify any potential threats to pupils' welfare and wellbeing. School has appropriate filtering and monitoring tools in place and have the right to monitor all devices and activity when and where necessary (See Filtering above).

REPORTING & CONTACT DETAILS
In the event of a Cyber Incident, please refer to the **Data Protection and Data Breach Response Plan**.
And immediately inform the following:

Headteacher / Con-Ed (via admin@sandridge.herts.sch.uk)

For Data Breaches, please inform the Headteacher who will inform the Data Protection Officer.

APPENDIX A – NCSC 10 Steps to Cyber Security

