Children First Learning Partnership

Inspiring Excellence Together

THE CHILDREN FIRST LEARNING PARTNERSHIP

INFORMATION SECURITY AND ACCEPTABLE USE POLICY

The Information Security & Acceptable use Policy in respect of the Children First Learning Partnership has been discussed and adopted by the Directors in Dec 22 following consultation with all Local Advisory Boards	
Chair of Board:	*Mrs N Chell*
Responsible Officer:	*CEO – Mrs A Rourke*
Agreed and ratified by the Directors	*05.12.2022*
To be reviewed:	*December 2024*

Contents

1. Overview

Executive Statement

Protecting the MAT and individual school's data is the responsibility of all employees. Security of information continues to be a critical issue in today's environment due to various threat factors including error, fraud and cyber attacks

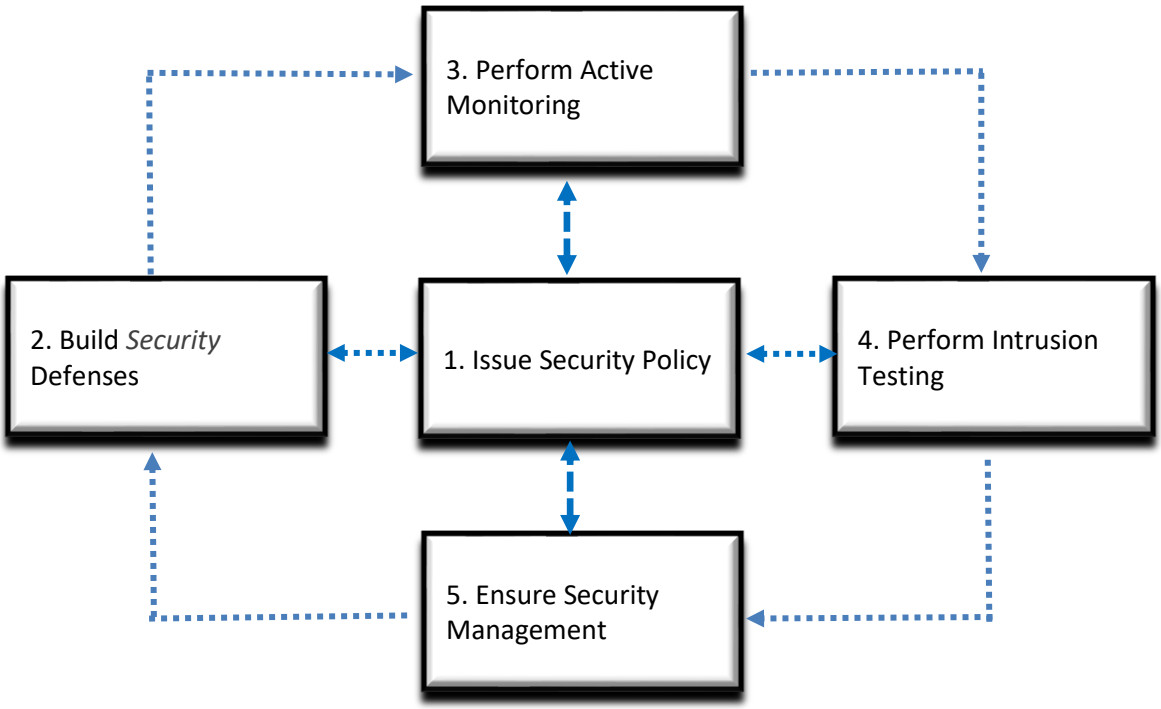
Information Technology (IT) is an increasingly integral part of the Schools's activities and is essential in the delivery of most services. Almost all school employees will use the school's Information Communication Technology (ICT) in the course of their duties.

This policy is designed to enable the School to:

- set guidelines and rules on the use of School ICT resources for our employees.
- establish clear expectations for the way all members of the school community engage with each other online
- support the school's policy on data protection, online safety and safeguarding.
- minimise legal and other risks associated with the use of technology
- ensure effective running of the school's business
- minimise the risk of disruption caused by computer viruses and inappropriate use of IT; and
- support the school in teaching pupils safe and effective internet and ICT use.

2. Information Security Governance

The CEO has overall accountability for information security within the MAT/Schools and for enforcing the policy. In this capacity the CEO can delegate the functions related to this role as appropriate, but still remains ultimately accountable



Issue Security Policy

Based on risk assessments performed throughout the Schools/MAT of the perceived threats to sensitive company assets an information security policy is created. Its key purpose is to document the controls, policies and guidance, as applicable to addresses the identified risks and associated threats

Build Security Defences

Once the risks have been identified, defences are implemented, some of these defences take on the form of security solutions. These solutions can have the ability to block, detect and/or prevent a risk from being exploited, Examples of these would be firewalls, anti-virus software, host or network intrusion prevention. Other forms may be more procedural in nature, Change management, safe storage of printed documents etc

Perform Active Monitoring

Once defences have been put into place, logs for these defence solutions are reviewed for potentially unauthorized or unexpected events. These events are then acted upon but IT or IT Security resources, data or system owners in accordance with the perceived severity.

Perform Intrusion Testing

Controls implemented to protect sensitive information resources must be periodically tested to ensure appropriateness and effectiveness

Ensure Security Management

Security management is the culmination of the whole program. It ensures that all of the necessary assets are accounted for, including information assets: that appropriate policies and procedures have been developed and documented to protect these assets. Furthermore, it ensures that the appropriate procedures such as information classification, risk assessment and risk analysis exist and are effective in identifying threats. This assessment is typically performed as internal security and internal audit.

3. Definitions

ICT facilities – includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services and any device system or service which may become available in the future which is provided as part of the ICT service.

Users – anyone authorised by the school to use the ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

Personal use – any use or activity not directly related to the users employment, study or purpose.

Authorised personnel – employees authorised by the school to perform systems administration and / or monitoring of the ICT facilities.

Materials – files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs.

Monitoring of school network and use of ICT facilities

The school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, the monitoring of:

- Internet sites visited
- Email accounts
- Telephone calls

- User activity / access logs
- Any other electronic communication

The school Systems including the internal and external e-mail system is monitored using Securus monitoring to ensure that the system is not being abused, to ensure:

- Ensure compliance with School/MAT Policies and for other lawful purposes
- Protect personal property and safety
- Protect information resources and property
- Ensure no illegal, unauthorized or non-permitted activity or information is transmitted stored or used on the computing resources

Unacceptable Use

The following is considered unacceptable use of the school's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings (see Sanction section below).

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth-produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering mechanisms

- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic or discriminatory in any other way

Exceptions from unacceptable use

Where the use of school ICT facilities (on the school premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the headteacher's discretion. A request for exemption would be done in writing to the CEO.

Sanctions

Staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies on staff code of conduct, staff social media code of conduct and staff disciplinary policy. These policies can be found here

www.childrenfirstlp.org.uk/policies

Breaches of this policy may result in disciplinary action up to and including dismissal. Breaches may also result in prosecution under the Computer Misuse Act 1990 and may lead to prosecution of the school and the individual concerned and / or civil claims for damages. Breach procedure is detailed in the Data Protection Policy

If you are unsure about how a rule or requirement applies, then discuss with the Head Teacher.

The MAT/School reserves the right in its sole discretion and without prior notice to remove from computing resource any material it views as offensive, inappropriate, improper or potentially illegal.

Except to the extent required by the MAT/School privacy policy, Employees should have no expectation of privacy associated with the information they store in or send through computing resources. Computing resources are the exclusive property of the School/MAT, and it reserves the right to examine all information stored in, or transmitted by, any computing resource

4. Software and Virus protection

The School adheres strictly to software licence agreements.

- Staff should not load any software onto the school systems or school laptops.
- Users should not copy software nor use unlicensed copies of software.
- Care should be taken to prevent and detect the introduction of viruses and other malicious software by adhering to this policy.

However, if you suspect a virus on any School equipment:

- Inform the school ICT Co-ordinator or Headteacher so that the school's ICT contractor can be informed.
- Unplug the network cable to isolate the PC
- Prevent anyone from using the PC.

5. Asset Register

All hardware will be recorded on the MAT asset register, using the serial number of the item, location and asset number.

6. Ownership Rights

All information and files created, received, stored or sent while on school business or using school facilities form part of the school's corporate records and remain property of the school.

7. Staff (including governors, volunteers and contractors)

Staff will be provided with a unique log in / account information and passwords that they must use when accessing the school's ICT facilities.

Use of email

- The school provides each member of staff with an email address
- This email account should be used for work purposes only.
- All work related business should be conducted using this school email address.
- Each user is responsible for the context of all text, audio and images that they send.
- No email or other electronic communications may be sent which misrepresents the sender as anyone else.
- The email service should not be used for transmitting, accessing, retrieving or storing any communications of a discriminatory or harassing nature or that are racist, offensive, obscene, pornographic, or sexually explicit. This applies to both business and personal use.
- Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.
- If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information the user must not make use of or disclose that information.
- If staff send an email in error which contains the personal information of another person they must inform the Headteacher immediately and follow the breach procedure.
- The sending or forwarding of chain letters or other unauthorised mass mailings, regardless of the subject matter, is not allowed.
- Treat suspect email or that from a dubious source with caution. Do not reply or forward (even to ICT) a message if there is any doubt. Similarly, do not open attachments or click on web links on suspect emails, as this could activate computer viruses or other malicious processes
- The sending of unwanted messages can constitute harassment. Careless use of language can lead to a bullying tone and can also be considered harassment.
- Do not send (or forward) email containing derogatory statements, potentially libellous, defamatory, comments likely to cause offence, gossip, hoaxes, or jokes to others inside or outside the school or MAT

Personal Use

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Headteacher may withdraw permission / restrict access at any time. Personal use is permitted provided that such use:

- Does not take place during teaching time
- Does not constitute unacceptable use

- Takes place when no pupils are present
- Does not interfere with their jobs or prevent other staff and pupils from using the facilities for work or educational purposes
- Staff should not use the school's ICT facilities to store personal non work information or materials (such as music, videos and photos).
- Access to gambling, pornographic sites and sites of a similar nature, is not allowed under **any** circumstances.
- Staff indicating their affiliation with the School, e.g. via an email address, or any other identifier, on social networking sites or other non-work related sites, must clearly indicate that the opinions expressed are their own, and not necessarily those of School or MAT. The school's guidelines on social media should be followed.
- The School does not accept liability for any loss or damage arising from use of the Internet to make personal financial transactions.

Mobile phones / Own devices

If mobile phones are brought into school they must be turned off and be put away during school hours. They can be switched on during break times in the designated areas which are the staffroom and the school office provided that no children are present. (Please also refer to the school Health and Safety Policy and safeguarding Policy.)

On school visits, staff are required to be contactable on their personal mobile phones. Under no circumstances, however, should any recording equipment on the mobile phone be used to take photographs/ videos of children. School cameras / IPads are provided for this purpose and should be taken on visits. This applies also to parents and volunteers who may be accompanying visits.

Remote Access / Mobile working

We allow staff to access the school's ICT facilities and materials remotely.

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on site.

- Equipment should be signed in and out of school using the ICT Security book which can be found in the school office.
- Always ensure that equipment and media are powered off when left unattended and preferably locked away.
- If carried by vehicle the equipment must be locked out of sight. It should not be left in an unattended vehicle for any length of time e.g. overnight.
- Only encrypted USB sticks / drives should be connected to school computers / laptops and password protection enabled.

User Password Security

The allocation of passwords shall be controlled through a formal management process using Evolve IT Support. The process should involve logging requests through Evolve IT ticket system to ensure it is auditable.

All computing resources that are connected, permanently or intermittently, to internal communications networks must have a strong password-based access control system

Passwords are an essential component to the security of the School/MAT information resource

Users should follow good password practices:

- A password should be at least seven characters in length.
- Contain characters from three of the four categories: uppercase; lowercase; 0 through 9; and special characters
- Not contain two of the same characters consecutively.
- Be difficult for anyone else to guess.
- Be kept confidential.
- Must not be written down in a place where unauthorized persons may discover them
- Be changed regularly.
- Administrator passwords that are set initially must be set in such a way that the user is forced to changed when logging in for the first time
- Password changes should be enforced every 90 days.

Users must 'log out' of systems fully or use the 'lock computer' command when leaving a workstation unattended.

Printer/scanning and copier security- All staff are expected to adhere to the same log out procedures as above when using a printer/copier /scanner. Alongside this staff must ensure no confidential documentation is left on any printer/copier or scanner when not in use.

Clear desk policy- All staff are expected to adhere to a clear desk policy ensuring no confidential documentation is left accessible to unauthorised staff or visitors and that all identified storage cabinets are locked at all times.

Physical security- All school sites have clear guidelines to ensure onsite security is a priority. A rigorous signing in procedure is in place including the expectation that all staff wear clear identification badges and visitors' identities alongside their DBS's are checked prior to access to school sites

Health & Safety

All employees have responsibility for Health & Safety in the workplace and this will be reflected in the manner that IT is used. Employees and managers are expected to ensure that the use of technology in their areas complies with the provisions of Health and Safety legislation and that the presence of technology in the office is not a cause for concern.

There are specific requirements for Display Screen Equipment (DSE) users and so far as the school is concerned an employee falls within the requirements of the DSE regulations if they use equipment for continuous spells of an hour or more (on average) every day. All such employees are required to complete a DSE risk self assessment and DSE training annually.

8. Pupils

Computers and equipment in the school's ICT suite / classroom based are available to pupils only under the supervision of staff.

Pupils will be provided with accounts linked to the various online learning platforms that school uses. These platforms may be accessed outside school.

Unacceptable use of ICT

The school will sanction pupils, in line with the behaviour policy if a pupil engages in any of the following at

- Using ICT or the internet to bully or harass someone else
- Access to gambling, pornographic sites and sites of a similar nature, is not allowed under **any** circumstances.
- Causing intentional damage to ICT facilities or materials.
- Using inappropriate or offensive language

If pupils bring a mobile phone to school it must be switched off and handed into the school office on arrival at school, for safe keeping. Pupil should collect their phone at the end of the school day.

9. Document change log

Date	Details of change / section number	Approved
27.10.22	P5 unacceptable use definition- through to sanction section added to provide additional guidance for all members of our school community.	
27.10.22	P9- Printer/scanner/copier use/clear desk policy, physical security sections added for further clarity	
27.10.22	P5 reference to Smoothwall removed and replaced with Securus	