The Children First Learning Partnership

Information Security Acceptable Use policy

(Version 1)

The Information Security Acceptable Use Policy in respect of the Children First Learning Partnership has been discussed and adopted by the Directors Board.

Chair of Board:	Mrs N Chell
Responsible Officer:	CEO – Mrs A Rourke
Agreed and Ratified by the Directors Board on:	21.05.2026
To be reviewed:	May 2026

Contents

1. Executive Statement 3
2.Purpose 3
3. Scope of the Policy 3
4. User responsibilities 3
5. Leadership Responsibilities 4
6. Definitions 5
7. Software and Virus Protection 6
8. Asset Register 6
9. Staff Responsibilities 8
10.Pupils 10
11. AI Tools Usage Rules 11
12. Policy review 12
13.Regulatory Foundations for this Policy 12

1. Executive Statement

Protecting the Children First Learning Partnership's (CFLP) data, digital infrastructure, and online environment requires all staff, governors, volunteers, contractors and authorised users to act responsibly and in line with updated 2025–2026 statutory expectations. This includes compliance with the Department for Education (DfE) Digital and Technology Standards, Cyber Security Standards, Filtering and Monitoring Standards, and current UK GDPR obligations.

2.Purpose

This Information Security & Acceptable Use Policy establishes the behaviours, technical controls, governance duties, and user responsibilities necessary to:

• Safeguard all school and trust information systems, devices, and data.
• Meet DfE expectations for cyber security, network management, filtering, monitoring, and secure data handling.
• Reduce risks associated with cyber-attacks, data breaches, insider threats and misuse of technology.
• Support compliance with UK GDPR, the Data Protection Act 2018, and the Data (Use and Access) Act 2025.
• Ensure safe use of online systems and digital tools by staff, pupils and other authorised users.

3. Scope of the Policy

This policy applies to all authorised users of CFLP ICT systems, including staff, governors, volunteers, contractors, visitors and pupils. It covers usage of:

• Trust and school networks, MIS systems, cloud platforms and communication tools.
• Trust-owned devices and authorised personal devices used for work purposes.
• Data, information assets, digital content, email, cloud storage, collaboration platforms and online learning systems.

4. User responsibilities

All users MUST:

- ✓ Read and comply with this policy before accessing CFLP systems.
- ✓ Complete mandatory annual cyber security, safeguarding and data protection training.
- ✓ Follow trust procedures for reporting incidents, suspected breaches or unsafe digital behaviour.
- ✓ Use school systems only for authorised and lawful purposes.
- ✓ Protect passwords, accounts, and devices in line with trust security standards.

Users MUST NOT:

⊗ Attempt to bypass filters, monitoring tools, or security controls.
⊗ Access or share information they are not authorised to view.
⊗ Introduce unsupported devices, unapproved software, or unsafe digital tools.
⊗ Use AI tools to process personal or sensitive pupil data without authorisation.

5. Leadership Responsibilities

Senior leaders, including the CEO and trust board, are accountable for ensuring governance structures, technical controls, risk management processes, and compliance monitoring are in place to uphold this policy.

Information Security Governance

The CEO retains ultimate accountability for information security across CFLP, in line with updated DfE Digital and Technology Standards (2025–2026), including cyber security governance, asset management expectations, and filtering and monitoring oversight.

Leadership Accountability

• The CEO ensures appropriate governance structures and risk management processes are in place.
• Trust boards must review cyber security posture and filtering/monitoring arrangements annually.
• Roles and responsibilities must be clearly assigned for managing filtering, monitoring, ICT systems, data protection and cyber security compliance.

Core Governance Duties

• Maintain a Trust-wide information risk register, reviewed termly.
• Ensure completion of annual cyber security training for all staff, governors and volunteers.
• Maintain an up-to-date Information Asset Register (IAR) aligned with DfE templates.
• Ensure Data Protection Impact Assessments (DPIAs) are conducted for new systems, high-risk processing, cloud services and AI tools.

Monitoring & Assurance

• Logs from filtering, monitoring, firewalls, antivirus, and intrusion detection systems must be reviewed regularly.
• Governing bodies must receive termly assurance updates on cyber security, data protection and online safety.
• Annual review of filtering and monitoring provision is mandatory.

Security Testing & Continuous Improvement

• Internal and external security testing must be conducted periodically, including vulnerability scanning and penetration testing.
• Lessons learned from incidents must inform updates to technical controls and policies.
• Business continuity and disaster recovery plans must account for digital infrastructure, aligned with DfE requirements.

6. Definitions

ICT Facilities – All digital systems, hardware, software, cloud platforms, network services, filtering and monitoring tools, and any future digital technologies provided by CFLP.

Users – Any individual authorised to access CFLP ICT systems, including staff, pupils, governors, volunteers, contractors, visitors and third-party service providers.

Information Asset – Any item of data or information (digital or physical) that has value to CFLP. This includes pupil records, staff data, safeguarding information, curriculum materials and system configurations.

Information Asset Owner (IAO) – A designated member of staff responsible for ensuring the security, accuracy and appropriate use of a specific information asset.

Personal Data – Any information relating to an identified or identifiable individual, as defined by UK GDPR.

Special Category Data – Sensitive personal data requiring enhanced protection, including health data, safeguarding records, ethnicity, religion, biometric data, etc.

Authorised Personnel – Staff with delegated permissions to administer systems, conduct monitoring, manage filtering, support technical security or handle sensitive information.

Filtering – Technology that blocks access to harmful or inappropriate online content in line with DfE filtering standards.

Monitoring – Technology and processes used to monitor user activity for safeguarding and cyber-security purposes, in line with DfE guidance.

Cyber Incident – Any event that threatens the confidentiality, integrity or availability of data or digital systems, including ransomware, phishing, unauthorised access or insider misuse.

AI Tools – Software or online platforms that use artificial intelligence, machine learning or automated decision-making techniques. These must not be used with personal data unless approved and covered by a DPIA.

Data Breach – Any breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

DPIA – A Data Protection Impact Assessment required for high-risk processing, including new systems, cloud services, AI tools and monitoring technologies.

7. Software and Virus Protection

Software Licensing and Compliance

• All software used on CFLP systems must be fully licensed and approved by authorised ICT personnel.
• Users must not install, modify or remove software without explicit authorisation.
• Only trusted, approved applications may be used on Trust devices, including staff laptops and any device accessing Trust data.

Protection Against Malware and Viruses

• All Trust devices must run centrally-managed antivirus and endpoint protection software.
• Automatic updates must remain enabled at all times to ensure devices receive security patches.
• Users must not disable, override, or interfere with security tools, including firewalls, antivirus, filtering and monitoring.

Handling Suspected Malware

If malware is suspected:
1. Immediately stop using the device.
2. Disconnect the device from the network (e.g., unplug network cable or disable Wi-Fi).
3. Report the issue to the ICT lead or Headteacher so it can be escalated to external IT support.
4. Do not attempt to remove malware yourself unless instructed by authorised personnel.

Software Updates and Patching

• All systems must be updated regularly, in line with DfE cyber security patching standards.
• Unsupported operating systems (e.g., Windows versions past end-of-life) must not be used.
• Devices that cannot be patched must be removed from Trust networks.

Use of External Media

• Only encrypted USB drives approved by CFLP ICT may be used.
• Personal USB devices must not be connected to Trust systems.
• External media must be scanned automatically before files are opened.

Cloud Applications and Online Tools

• Any new cloud service used for teaching, administration or data storage must be risk-assessed and approved.
• AI-based tools or online apps must not be used to process personal or sensitive data without a DPIA and explicit authorisation.

8. Asset Register

Purpose of the Asset Register

The CFLP Asset Register exists to ensure full visibility of all hardware, software, cloud services, and network-connected devices used across the Trust. It supports:
• Compliance with DfE cyber security standards.
• Accurate tracking of device status, lifecycle, warranty, and patching requirements.

• Identification of unsupported or non-compliant technology (including end-of-life operating systems).
• Assurance for safeguarding, data protection, and incident response processes.

Asset Register Requirements

• All hardware (computers, laptops, tablets, servers, networking equipment, printers, cameras, mobile devices) must be recorded with its serial number, asset ID, current user (if assigned), and physical location.
• All software, cloud services, and licensed applications must be documented, including renewal dates and data-processing responsibilities.
• Any changes to assets (additions, removals, loss, theft, damage, disposal) must be reported immediately to the office manager for recording.
• The Asset Register must be reviewed at least annually to ensure accuracy.
• Devices reaching end-of-life or no longer supported by vendors must be removed from the network in line with national cyber security expectations.

User Responsibilities

• Staff must not remove equipment from the premises without signing it in/out through the formal ICT equipment log.
• Any IT equipment used remotely (e.g., staff laptops) remains the property of the Trust and must be returned upon request.
• Users must promptly report misplaced, damaged, or malfunctioning assets to authorised personnel.

Disposal and Replacement

• Disposal of ICT equipment must comply with data protection requirements and secure-wiping standards.
• Assets must only be disposed of by authorised ICT staff or contracted providers.
• Replacement planning must take account of cyber security, safeguarding, and DfE lifecycle recommendations.

6. Ownership Rights

Ownership of Information and Systems

• All information, digital content, communications, system configurations, and files created, received, stored or transmitted using CFLP ICT systems remain the property of the Children First Learning Partnership.
• This includes documents, emails, photographs, recordings, cloud-stored files, metadata, monitoring logs, and any derivative work created using Trust platforms or devices.

Authority and Control

• CFLP retains the right to access, review, audit, archive or delete any data or digital activity stored on its systems, in line with data protection legislation and safeguarding responsibilities.
• Users must not claim intellectual ownership over Trust-produced materials, digital resources, lesson content, or administrative documents created during employment.
• All data created during employment or during authorised access forms part of the Trust's corporate

record.

Use of Personal Devices

• Any Trust data accessed or stored on personal devices remains the property of CFLP.
• Users must ensure such data is protected through encryption, secure storage, and authorised access only.
• Upon ending employment or permissions, users must delete all Trust data from personal devices and return any files as instructed.

Third-Party and Cloud Services

• All data processed through third-party platforms (e.g., cloud systems, MIS systems, safeguarding tools, communication apps) remains owned by CFLP.
• Third-party providers act only as data processors and must comply with relevant data protection requirements.

When Access Ends

• When a user leaves the Trust or no longer requires system access, their accounts will be disabled and their data reviewed for retention or secure deletion.
• No data belonging to CFLP may be taken, stored, or transferred without explicit written authorisation.

9. Staff Responsibilities

All staff, including governance team members, volunteers, contractors and temporary workers, play a critical role in maintaining the security, integrity and lawful use of the Children First Learning Partnership's information systems. This section outlines mandatory responsibilities in line with updated DfE Cyber Security Standards (2025–2026), KCSIE 2025 requirements, the UK GDPR, and the Data (Use and Access) Act 2025.

Account Access and Authentication

• Staff must use their unique login credentials and must not share passwords with any other individual.
• Multi-factor authentication (MFA) must be enabled on systems where available, including email, MIS and remote access systems.
• Passwords must meet Trust security requirements and be changed at mandated intervals. Default or weak passwords must not be used.

Use of Email and Communication Systems

• All work-related communication must be conducted using the authorised school email account.
• Staff must ensure emails containing personal, sensitive, safeguarding or confidential data are encrypted and handled in accordance with data protection requirements.
• Staff must not forward chain letters, inappropriate messages, unapproved mass mailings or any content that could breach safeguarding, copyright, or data protection legislation.
• Suspect phishing emails or malicious messages must be reported immediately following the incident

reporting procedure.

Acceptable Use of ICT Facilities

• ICT facilities may not be used for personal financial transactions, storing personal media or accessing blocked or prohibited sites.
• Personal use must not interfere with work duties and may only occur during non-contact times and never in the presence of pupils.
• Staff must not install software, browser extensions, or applications without authorisation.

Cyber Security Responsibilities

• Staff must complete annual cyber security training, including phishing awareness, password hygiene, and secure data handling.
• Any suspected cyber incident—including suspicious login attempts, unexpected system behaviour or suspected breaches—must be reported immediately.
• Staff must not use unsupported operating systems or devices for school work.

Use of AI, Digital Tools and Online Platforms

• Staff must ensure that any use of AI, automated decision-making tools, or digital applications involving pupil or staff data is approved following all expectations detailed in the CFLP AI Policy and covered by a DPIA.
• AI tools must not be used to process sensitive or identifiable pupil information unless authorised and compliant with UK GDPR and Data (use and access) Act (DUAA) safeguards.
• Staff must explain when AI is used in decision-making processes that affect individuals.

Data Protection and Confidentiality

• Staff must follow all data handling procedures, ensuring personal data is stored securely and accessed only when necessary for their role.
• Personal information must not be removed from school systems unless authorised and protected through encryption.
• Staff must follow secure transfer requirements, including the statutory 5-day transfer window for safeguarding files.

Remote Working and Device Security

• Devices must be transported securely, locked out of sight in vehicles, and never left in unattended vehicles overnight.
• Only encrypted USB drives may be used.
• All devices must be locked when not in active use.

Mobile Phone Use

• Personal mobile phones must be turned off and stored away during the school day unless in approved staff-only areas.
• Staff must not use personal devices for taking photographs or videos of pupils under any circumstances.

Incident Reporting

• All incidents, misuse, security concerns, or potential breaches must be reported immediately to the Headteacher and/or Office Manager.
• Failure to report incidents may result in disciplinary action.

Professional Conduct Online

• Staff must follow all social media and online behaviour policies.
• When identifying as an employee online, staff must clarify that views expressed are personal.This section reflects updated DfE filtering and monitoring standards (2024–2026) and KCSIE 2025 online safety expectations.

10.Pupils

Access and Supervision

• Pupils may only access ICT facilities under direct staff supervision.
• All pupil activity must be monitored in line with DfE filtering and monitoring requirements.
• Pupil access to online learning platforms must follow age-appropriate safety controls.

Online Safety Expectations

• Pupils are taught how to stay safe online in accordance with relevant KCSIE Guidance.
• Pupils must report concerns about harmful or inappropriate content immediately.
• Pupils must use age-appropriate digital platforms approved by the Trust.

Unacceptable Use by Pupils

The following behaviours are strictly prohibited:
• Using ICT to bully, harass or harm others.
• Accessing gambling, extremist, pornographic or otherwise harmful sites.
• Attempting to bypass filtering or monitoring tools.
• Damaging ICT equipment or interfering with security settings.
• Using AI tools to create harmful, inappropriate or unsafe content.

Mobile Phones

• Pupils must switch off mobile phones on arrival.
• Phones must be handed in to the office and collected at the end of the day.
• Use of personal devices during the school day is not permitted.

Account Security

• Pupils must keep their login details secure and must not share passwords.
• Any attempt to access another user's account will result in sanctions.

Sanctions

• Breaches of this section will be managed through the school's behaviour policy.
• Serious incidents—including hacking attempts—may be escalated to safeguarding leads or external agencies.

11. AI Tools Usage Rules

The Children First Learning Partnership recognises that artificial intelligence (AI) tools have the potential to support teaching, learning, and administrative efficiency. However, their use introduces new data protection, ethical, and safeguarding risks. The following rules apply to all staff, governors, volunteers, contractors, and pupils (where appropriate).

Approved AI Tools Only

• Staff may only use AI tools that have been formally approved by the Trust and are covered by a current Data Protection Impact Assessment (DPIA).
• No personal, pupil, staff, or confidential data may be processed using unapproved third-party AI platforms.

Use of Personal Data

• AI tools must not be used to analyse, generate, store, or process personal data unless explicitly authorised and documented.
• Sensitive data—including safeguarding information—must never be entered into AI systems.

Automated Decision-Making (ADM)

• Staff must not use AI systems to make or inform decisions that affect pupils or staff without prior authorisation and a valid DPIA.
• Individuals affected by ADM must be informed about how decisions are made and have a right to challenge outcomes.

Transparency and Accountability

• Staff must disclose when AI has been used to produce or support work that forms part of official school communication or decision-making.
• AI-generated content must be reviewed for accuracy, bias, and appropriateness before use.

Safeguarding and Ethical Use

• AI must not be used to create, alter, or manipulate images, audio, or video involving pupils or staff.
• Deepfake content, synthetic media, or misleading material is strictly prohibited.

Cyber Security Considerations

• AI tools must be accessed via secure accounts with multi-factor authentication where possible.
• Staff must report any AI-related security incidents, suspicious behaviour, or unexpected model outputs immediately.

Pupil Use of AI

• Pupil use of AI tools must be supervised and linked to curriculum aims.
• Pupils must receive guidance on safe, ethical, and responsible use of AI technologies.

Prohibition of AI for Behavioural Prediction or Surveillance

• AI must not be used for monitoring pupil behaviour, predicting future behaviour, or analysing

emotional states.
• Facial recognition systems are not permitted unless approved by the Trust Board and accompanied by a DPIA.

These rules reflect developments in the Data (Use and Access) Act 2025 and updated ICO guidance on automated decision-making, AI transparency, and responsible system deployment.

12. Policy review

The policy will be formally reviewed:

• Annually

An annual review allows the Trust to reflect on developments in Acceptable Use and Information Security, update processes in line with national guidance, evaluate outcomes from school practice, and ensure all content remains up to date and legally compliant.

• After any significant incident involving Information Security or Acceptable Usage,

If an acceptable use, information security, data-protection or cybersecurity concern arises, the policy will be reviewed immediately. This ensures lessons are learned, risks are addressed, and controls are strengthened without delay.

13.Regulatory Foundations for this Policy

This section incorporates the latest 2025–2026 regulatory changes, including:
• Updated DfE digital standards, including enhanced filtering and monitoring, expanded requirements for asset registers, and upgraded cyber security expectations.
• National updates on cyber incident response and reporting pathways (including replacement of Action Fraud with Report Fraud).
• ICO guidance on children's privacy, information security, subject access requests (SARs), and strengthened oversight under the Data (Use and Access) Act 2025.
• New AI and automated-decision making (ADM) safeguards from the ICO's 2025–26 AI and biometrics strategy.

Version Control

Version	Date	Amendment	By
1	27/03/2026	New version	CEO