Information Security and Acceptable Use Policy

Responsible Committee	CLPT Finance & Operations Committee
Date Approved by Committee	12th December 2025
Implementation Date	12th December 2025
Next Review Date	Autumn Term 2027
Policy Owner	Laura Austen, Connor Millington-Lock

This document has been created to support the mission, values and beliefs of the Creative Learning Partnership Trust:

Our mission.

Creating **transformational** educative opportunities; promoting **social justice**; unlocking individual **freedom**

Our values.

Integrity
Courage to do the right thing, taking time to care.
Speaking and acting truthfully, fairly and upholding universal, moral principles.

Collaboration.
Working together, enabling each other.
Working with others to achieve strategic direction and to develop mutual trust and respect.

Dedication.
Committed to supporting and improving.
Showing commitment to and responsibility for strategies and goals.

Kindness.
Thinking of others and acting with compassion.
Demonstrating intentional actions to show care, respect and empathy to others.

Innovation.
Using expertise and research to transform.
Taking a proactive approach to problem solving , showing creativity, forward thinking and adaptability.

Understanding.
Openness, listening and valuing one another.
Actively listening to others to gauge the perspectives and needs of others within relevant context.

C — CREATIVE.

Creativity is at the heart of how we achieve exceptional educational outcomes. It drives innovation and empowers us to transform new and original ideas into reality, enriching the learning experience for every child.

L — LEARNING.

Learning is at the core of all we do. We are relentless in our commitment to ensuring that every child within our care achieves outcomes that truly reflect their potential and aspirations.

P — PARTNERSHIP.

Collaboration and **partnership** are key to continuous improvement. By working together, we create an inclusive, supportive, and responsive organisation that listens and learns from all voices.

T — TRUST.

Trust is the foundation of our culture. It permeates every aspect of our schools and organisation, creating confidence, integrity, and building strong relationships across our entire community.

Mission Statement

The Creative Learning Partnership Trust (CLPT) has a duty to ensure the safety and security of all pupils, families, staff and governors within our schools. Therefore, Information Security is crucial within our setting and at all times, we will apply the principles of confidentiality and integrity when considering availability of data.

In order to promote Information Security, this policy also outlines our commitment to Acceptable Use of ICT. Responsible use of ICT helps us all to protect CLPT against information breaches.

We acknowledge Article 5 of the UK GDPR requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The Creative Learning Partnership Trust believes it is essential to identify and outline the roles and responsibilities of all those involved in the procedures and arrangements that are connected with this policy.

Scope

Information security applies equally to and is the responsibility of everyone at all levels.

Data is any information that is considered to be personal, sensitive or valuable to individuals or the school. CLPT reserves the right to monitor staff network use and revoke access if they are deemed to be in breach of the AUP and Guidelines. Members of staff who choose to ignore the acceptable use policy and guidelines may face disciplinary action. Breach of these or any related policy could result in criminal or civil actions being brought against you.

Specific Responsibilities

Data in your possession becomes **your responsibility** - you must keep it secure and in your possession at all times. The principle of 'Complete the task, return the data' is to be applied at all times.

- It is the role of the Headteachers, with support from the nominated governor and the IT lead, to ensure e-safe practices throughout school. They must ensure that ICT policies are implemented, monitored and up to date.
- Staff are responsible for ensuring that everyone in school (staff and pupils) adheres to the policies set. They should instil online safety standards across the school through best practice. Staff are encouraged to raise all concerns relating to ICT misuse as and when they occur.
- All visitors should sign an online safety agreement on arrival in schools if they wish to use the school network, confirming that they have completed the NCSC “Cyber Security training for school staff” within the last 12 months. They should use the network responsibly for the purpose of their task and no more.
- The wider community (parents and carers) are urged to support online safety. Some examples of this are through:
    - The school websites have an icon that highlights and links users to report online material promoting terrorism or extremism.
    - The school websites (under the safeguarding section) provide links to Staffordshire Safeguarding Children's Board and NSPCC online safety information.
    - Sharing key information in the school newsletters.

The Local Governing Board (LGB) has:

- appointed a member of staff to be responsible for ICT in conjunction with the trust Head of IT;
- delegated powers and responsibilities to the Headteacher to ensure all school personnel and stakeholders are aware of and comply with this policy;
- responsibility for ensuring full compliance with all statutory responsibilities;

- responsibility for ensuring that the school complies with all equalities legislation;
- responsibility for ensuring funding is in place to support this policy;
- responsibility for ensuring this policy and all policies are maintained and updated regularly;
- responsibility for ensuring all policies are made available to parents;
- made effective use of relevant research and information to improve this policy;
- responsibility for the effective implementation, monitoring and evaluation of this policy.

Role of Headteachers and Senior Leadership Teams

The Headteachers and the Senior Leadership Teams will:

- ensure all school personnel are aware of and comply with this policy;
- ensure all school personnel sign and date the 'Acceptable Use Agreement' (Appendix 1);
- work closely with the safeguarding governor;
- provide leadership and vision in respect of equality;
- provide guidance, support and training to all staff;
- make effective use of relevant research and information to improve this policy;
- monitor the effectiveness of this policy;
- lead the development of this policy throughout the school;
- devise and update acceptable use guidelines when appropriate;
- keep a log of all ICT equipment used by school personnel (delegated responsibility to CLPT IT Department);
- liaise with CLPT IT Department to provide staff with correct software (encryption, antivirus, firewall etc.);
- keep up to date with new developments and resources;
- undertake risk assessments when required;
- ensure staff understand their roles and responsibilities in relation to filtering and monitoring systems.

Maintaining the Security of the School's IT Network

The Chief Operating Officer, working with the Head of IT and Headteachers, is responsible for maintaining the school network. The Chief Operating Officer, working with the Head of IT and Headteachers, must ensure that virus protection is up to date and appropriate backups are conducted daily. The Headteacher/DHT is also responsible for monitoring network use and policy compliance by all users.

Role of Nominated Governors (LGB)

The Nominated Governor will:

- work closely with the Headteacher and DHT;
- ensure this policy and other linked policies are up to date;
- ensure that everyone connected with the school is aware of this policy;
- attend training related to this policy;
- report to the Governing Body.

Role of the Designated Safeguarding Lead (DSL)

The Designated Safeguarding Lead will:

- take lead responsibility for safeguarding and child protection (including online safety);
- understand the filtering and monitoring systems and processes in place;
- be the first point of contact for staff who have concerns about online safety or ICT misuse;
- work with the Headteacher/DHT to ensure online safety concerns are addressed promptly;
- liaise with local authority children's social care and other agencies as appropriate;
- ensure staff understand how to report concerns to the DSL;
- maintain records of online safety concerns and incidents;
- ensure online safety is embedded in the child protection policy.

Role of School Personnel

School personnel will:

- sign, date and comply with all aspects of this policy;
- make themselves aware of all other linked policies;
- encourage and remind other staff to follow the acceptable use guidelines;
- implement the school's equalities policy;
- report and deal with all incidents of discrimination;
- attend appropriate training sessions on induction and at least annually;
- report any concerns they have on any aspect of the school community;
- understand that all data stored on the school server is owned by the school and is not to be removed without permission;
- report all online safety concerns to the DSL or Headteacher/DHT immediately;

- understand their roles and responsibilities in relation to filtering and monitoring systems.

Overview

- Staff must receive online safety and child protection training (including understanding of filtering and monitoring systems) at induction and at least annually through updates (e.g. via email, e-bulletins, staff meetings).
- Staff must make themselves familiar with all school policies and linked policies.
- All users of technology must receive and complete the NCSC "Cyber Security training for school staff" annually and be able to evidence this.
- New staff should receive relevant policies as part of their induction.
- Staff must understand their roles and responsibilities in online safety and data protection.
- Staff must report misuse of the school network and equipment immediately to the DSL or Headteacher/DHT.
- Staff must report theft, loss or damage to/of data or equipment immediately to the Headteacher/DHT.
- Staff must ensure that online safety forms part of their classroom culture.
- Staff must promote acceptable ICT behaviour when working with children.
- Staff should preview ICT materials (websites, videos, PowerPoints etc.) before use with pupils.
- CLPT and all associates have a collective responsibility to promote online safety through their own actions.
- Online safety should be a constant theme, as appropriate to the children's age and stage of development, during IT use.
- Staff, parents and children should be encouraged to discuss and report online safety concerns so that issues can be addressed and best practice is shared.
- Staff must ensure children (where appropriate) know how to report abuse by speaking to the DSL or any member of staff (who will escalate the concern to the DSL/Headteacher).
- We will educate parents through sign-posting on the school website.

Aims

- To ensure school personnel are aware of all legislation relating to information security, data protection, computer use and misuse and copyright.
- To create a safe and secure information and ICT (Information Communication Technology) environment for each other.

- To ensure that anyone with access to information and the school network or loaned devices:
    1. understands that the school network use is filtered and monitored;
    2. understands they must comply with all policies and procedures relating to ICT;
    3. understands their roles and responsibilities in Online safety and Data Protection;
    4. receives a comprehensive online safety education programme appropriate to their role.
- To ensure all staff understand how filtering and monitoring systems work and their responsibilities in relation to these systems.
- To ensure ICT systems and practices are accessible and inclusive for all staff and pupils, including those with SEND.
- To prevent discrimination through ICT systems and online behaviour.

Filtering and Monitoring Systems

How Our Systems Work

All schools in The Creative Learning Partnership Trust use broadband provided through Exa Networks. This is a "filtered" internet service to minimise exposure to unwanted materials. We also use:

- **Securus** - monitors the whole school network automatically. All screen content and keyboard activity can be recorded if it is deemed to be a violation of policy.
- **Surfprotect** - controls access to web content and resources.

Staff Roles and Responsibilities

All staff must:

- Understand that all internet use is filtered and monitored;
- Know who to report concerns to if they identify issues with filtering or monitoring (Headteacher/DHT);
- Understand that monitoring is in place to keep children safe, not to monitor staff inappropriately;
- Be aware that the DSL has overall responsibility for understanding the filtering and monitoring systems;
- Report immediately if they accidentally access inappropriate material or if filtering systems fail;
- Understand that the Headteacher/DHT reviews monitoring reports regularly.

System Review and Updates

The Headteacher/DHT, working with CLPT IT Department, will:

- Review filtering and monitoring systems at least annually;
- Update systems in response to new threats or safeguarding concerns;
- Ensure systems are appropriate for the age and needs of pupils;
- Test systems regularly to ensure they are working effectively;
- Report to governors on the effectiveness of filtering and monitoring.

What to Do If Systems Fail

If staff identify that:

- Inappropriate content is accessible despite filtering;
- Monitoring systems are not working;
- There are gaps in protection;

They must report this immediately to the Headteacher/DHT who will liaise with CLPT IT Department to resolve the issue.

Monitoring of IT Systems

- The Headteacher or CLPT IT Department may, without prior notice, inspect or monitor any ICT equipment or peripheral (e.g. data, e-mail, texts or image) owned or leased by the school at any time under the Data Protection Act 2018 and UK GDPR, or to prevent or detect crime.
- Securus monitors the whole school network automatically. All screen content and keyboard activity can be recorded if it is deemed to be a violation of policy.
- Surfprotect controls access to web content and resources.
- Monitoring is conducted in accordance with the Data Protection Act 2018 and UK GDPR.
- Staff will be informed that monitoring takes place and the purposes for which it is conducted.

Security Incident / Breach Reporting

Concerns

Everyone connected with the school is encouraged to report online safety concerns immediately to the DSL or Headteacher/DHT for escalation. This includes concerns about:

- Inappropriate content accessed by pupils or staff;
- Online bullying or harassment;
- Child-on-child abuse online;

- Harmful online challenges or hoaxes;
- Inappropriate use of social media;
- Potential grooming or exploitation;
- Any other online safety concern.

Low-Level Concerns

A low-level concern is any concern - no matter how small, and even if no more than causing a sense of unease or a 'nagging doubt' - that an adult working in or on behalf of the school may have acted in a way that:

- is inconsistent with the staff code of conduct, including inappropriate conduct outside of work, and
- does not meet the harm threshold or is otherwise not serious enough to consider a referral to the LADO.

Examples of low-level concerns related to ICT use could include, but are not limited to:

- Using school ICT equipment for excessive personal use;
- Inappropriate comments on social media that don't meet the harm threshold;
- Minor breaches of acceptable use policy;
- Failure to follow data protection procedures on a single occasion.

Reporting Low-Level Concerns:

All low-level concerns should be reported to the Headteacher/DHT (or DSL if the Headteacher/DHT is the subject of the concern). The Headteacher/DHT will:

- Record the concern in writing, including details of the concern, context, and action taken;
- Decide on appropriate action (e.g. conversation with staff member, additional training, monitoring);
- Consult with the DSL where appropriate;
- Refer to the LADO if the concern meets the harm threshold;
- Review records regularly to identify patterns of behaviour.

Low-level concerns will be kept confidential, held securely and will comply with the Data Protection Act 2018 and UK GDPR. Records will be retained at least until the individual leaves employment.

Staff are encouraged to self-refer if they find themselves in a situation which could be misinterpreted or appears compromising.

Breaches of Policy

Any policy breaches are grounds for disciplinary action in accordance with the School Disciplinary Policy. Policy breaches may also lead to criminal or civil proceedings.

Incident Reporting

All security breaches (loss of equipment or data, unauthorised or misuse of ICT, theft of equipment or data) should be reported immediately to the Headteacher/DHT for escalation.

Any data breaches should be reported to the DPO in line with the procedure in the Data Protection Policy.

Password Security

- Use a strong password (the longer the better - minimum 8 characters including upper and lower case letters, numbers and symbol).
- Passwords should not be written down.
- Passwords should not be shared with anyone.
- Passwords should be changed every 3 months or if you feel they have been compromised.
- All school devices must be password protected.
- Passwords must never be Auto Saved to any devices.
- Staff must not use the same password for school and personal accounts.

Internet Use

All schools in The Creative Learning Partnership Trust use broadband provided through Exa Networks. This is a "filtered" internet service to minimise exposure to unwanted materials.

- Access to the internet, via cable or Wi-Fi, is only accessible if permission has been granted by the Headteacher/DHT or CLPT IT Department and the relevant documentation has been signed. This can be revoked at any time.
- Network use is monitored by the Headteacher/DHT with the help of Securus Monitoring Software.
- Staff must preview any internet resources before using them with pupils.
- Internet searches must be conducted responsibly at all times.
- If unsuitable material is discovered, turn off the computer screen (if you are with a child). When appropriate, log the site address and report it to the Headteacher/DHT. The site will then be blocked from future use.
- Anyone using the school network or Internet will not seek out offensive materials or information that is not relevant to them.
- Content should only be downloaded from sites where it is legal to do so.

- Staff should use the school ICT equipment and internet for school-related purposes. It should not be used for browsing for personal use.
- No personal information such as phone numbers and addresses should be given out over the internet. Arrangements to meet someone should not be made unless this is school/job related.
- Any member of the school personnel that uses illegal software or accesses inappropriate websites either in school or on any mobile devices provided by school faces dismissal.
- Staff must be aware of and report harmful online challenges and online hoaxes.
- Staff must be vigilant to child-on-child abuse that may occur online.

Email Security

- School correspondence must be sent via school accounts not personal emails.
- Emails must not contain inappropriate material.
- Always check that emails are addressed to the correct recipient.
- Sensitive data must not be sent by email unless it is securely encrypted.
- Think before you click - Do Not open emails if you do not recognise the sender or attachment.
- If you access school emails on a personal device you must ensure it is securely protected in accordance with this policy (password protected, etc.).
- School emails can be monitored and explored at any time if you are deemed to have breached policy.
- Emails should be marked as follows:

Public	**No need to mark public documents**
School Use	Not for release to the public
Restricted	Not for release to all staff
Confidential	Would cause serious damage if released

Remote Access Security

- Remember to lock or log off devices before you leave them (WINDOWS KEY+L if you leave your seat).
- When working on confidential information it should be carried out in a confidential environment (angle screens away from people, prevent 'shoulder surfing', encryption applied to documents, away from areas accessed by the general public, etc.).

Working From Home Security

We acknowledge that at times, it is necessary to take data home in order to fulfil one's role. However, it is necessary to put safeguards in place in order to protect the security of information. These are as follows:

- Lock paper records away when not in use.
- Ensure that any laptop data on is encrypted. The IT department can check this if you are not sure.
- Laptops should be correctly shut down after use to ensure encryption is activated.
- Do not allow family or friends to see school's data.
- Family and friends should not use school's ICT equipment.
- Paper records e.g. learning journeys should be signed in/out.
- Do not use removable storage devices of any kind e.g. USB Sticks, USB Hard drives, CDs

Mobile Device/Removable Media Protection

- School devices should only be used if you have been authorised to do so.
- Devices loaned by school should only be used by the individual they have been allocated to.
- Every device should be secured with a password and username where applicable.
- Remember to lock or log off devices before you leave them (WINDOWS KEY + L if you leave your seat).
- Loaned devices that may be taken from school should have sufficient levels of encryption. Staff should be aware of how to use this properly.
- Any loaned device allocated to you by school is your responsibility, it must:
    - Have the relevant password protection and encryption. If you are unsure ask the Headteacher/DHT.
    - Be secured safely and not left unattended at any time.
    - Only be used for work-related purposes, not personal.
    - Be cleansed of information that is not needed.
- School devices should never be connected to open Wi-Fi networks e.g. in a café or airport.
- When working on confidential information it should be carried out in a confidential environment (angle screens away from people, prevent 'shoulder surfing', encryption applied to documents, away from areas accessed by the general public, etc.).
- Any devices provided for class use (iPads, cameras, switches etc.) are the responsibility of the department. They must be stored securely, access should always be monitored.

- Staff are responsible for ensuring that loaned devices are regularly backed up with the help of the Headteacher/DHT. These backups need to be stored in a secure location.
- The Headteacher/DHT can recall or restrict access at any time to any school device for maintenance purposes. If you are requested to return a device this must be done promptly to reduce disruption.
- Do not use removable storage devices of any kind e.g. USB Sticks, USB Hard drives, CDs

Personal Devices and Mobile Phones

- Are not permitted in school unless express permission has been granted by the Headteacher.
- If permission has been granted they should be on silent and only used in designated staff areas.
- School is not responsible for loss or damage to personal devices brought into school by staff or children.
- If children have personal iPads, it is the responsibility of staff to make sure that it is only used with the individual and that the information that is recorded on the device only pertains to the individual.
- CLPT is not responsible for devices loaned to children via third parties.
- Staff must ensure personal devices used to access school systems (e.g. email) are password protected and comply with this policy.
- Staff must not store school data on personal devices unless explicitly authorised and appropriately encrypted.
- "Meta" AI wearable technology is strictly prohibited across all trust sites for staff, pupils and visitors.

Software

- Training should be available to all staff on software that is appropriate/required for their roles.
- Staff should be aware of what programs are available in school and how to use them effectively.
- Staff must not install any software on any school devices without express permission of the CLPT IT Department.
- Staff should ensure that when a device requires updates, these are implemented. Do not ignore the requests.
- Staff must not use unauthorised AI tools or generative AI applications on school devices without permission from the Headteacher/DHT.

- Any use of AI tools must be in accordance with school policies and with appropriate safeguards for data protection.

Digital Media

- Staff should only use photographic devices provided by school.
- Staff are responsible for ensuring the safety of these devices at all times.
- Staff must know which children have the relevant permissions relating to digital images. An up-to-date list is kept in the school office. If you are unsure, ask.
- Children's images should not be identified by name for any school activities.
- It is prohibited to take any form of digital media out of school without authorisation.
- When photos are used e.g. in the calendar, explicit consent has been sought.
- Images must be stored securely and deleted when no longer required in line with the school's retention schedule (see Privacy Policy).

Protective Marking

All data will be given a classification to determine how it is processed.

Public	**No need to mark public documents**
School Use	Not for release to the public
Restricted	Not for release to all staff
Confidential	Would cause serious damage if released

Secure Data Transfer

Secure Data Transfer will be used when transferring and receiving files from external sources. The preferred method of secure data transfer for sending files is OneDrive. Staff must:

- Only use approved secure file transfer methods.
- Never send confidential or sensitive data via unencrypted email.
- Verify recipient details before sending any data.
- Use password protection for sensitive documents where appropriate.

Backups

Data is backed up to the cloud once every day. Staff must:

- Ensure they save work regularly to the school network.
- Report any issues with backups immediately to the CLPT IT Department.
- Not rely solely on local device storage.

Printing/Scanning/Copier Security

- Confidential information must NOT be left in these devices.
- Staff should always try to reduce the amount of printing in school to a minimum where possible.
- When printing confidential documents you must:
    - Ensure that you have selected the correct printer.
    - Only print one copy of the document (extras can be photocopied if needed).
    - Collect the printing immediately.
- It is the responsibility of all staff to ensure that confidential documents are not left on or by the printers.
- Documents that you find must be handed to the owner or shredded.
- Confidential documents must be sent securely (via the 'hold' function or entering a PIN).

Social Networking

As a Condition of Service, all employees are expected to maintain conduct of the highest standard such that public confidence in their integrity is maintained. Care should be taken with the personal use of Social Networking Sites to ensure that the integrity of CLPT is maintained. Staff should use any social networking with extreme caution. Beware that what you post online can affect your professional position.

Staff must:

- Understand that under no circumstances should school pupils or parents, past or present, be added as friends or contacts.
- Understand that their role in school requires a high degree of professionalism and confidentiality.
- Be aware that any communications or content they publish that causes damage to the School, Trust, any of its employees or any third party's reputation may amount to misconduct or gross misconduct to which the School and Trust Dismissal and Disciplinary Policies apply.
- Understand that the right to freedom of expression attaches only to lawful conduct.
- Be aware that no communication of a professional nature should be made through social media. This relates to:
    - children;
    - anything that will bring the school or its associates into disrepute;
    - breach of confidentiality;
    - breach of copyright;
    - breach of data protection;

- offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion, belief or age;
- bullying;
- posting images that are discriminatory or offensive or links to such content.

All employees are advised to ensure that when setting up social networking sites they should make full use of the range of tools which enable the access to personal information to be restricted.

(See Staff Code of Conduct and Code Of Practice For Employees in the use of Social Networking Sites and Electronic Media)

Artificial Intelligence (AI) and Generative AI

The use of AI tools in education is increasing. Staff must:

- Only use AI tools that have been approved by the Headteacher/DHT.
- Understand that AI-generated content may contain inaccuracies and must be checked before use with pupils.
- Never input confidential or personal data about pupils, staff or families into AI tools unless they are approved and secure.
- Be transparent with pupils when AI-generated content is being used.
- Teach pupils about the appropriate and responsible use of AI tools.
- Be aware that AI tools may perpetuate bias and stereotypes.
- Report any concerns about AI use to the DSL or Headteacher/DHT.

Online Challenges and Hoaxes

Staff must be aware of harmful online challenges and online hoaxes that may put children at risk. Staff must:

- Stay informed about current online trends and challenges that may affect pupils.
- Report any concerns about pupils engaging with harmful online challenges to the DSL immediately.
- Teach pupils about the dangers of online challenges and how to stay safe.
- Work with parents to raise awareness of online challenges and hoaxes.
- Never share or promote information about harmful challenges, even in a warning context, as this may increase awareness and participation.

Child-on-Child Abuse Online

Child-on-child abuse can occur online as well as offline. This includes:

- Cyberbullying

- Sexual harassment and sexual violence online
- Sharing of nudes and semi-nudes (previously known as 'sexting')
- Online abuse in intimate personal relationships between peers
- Initiation/hazing type violence and rituals

Staff must:

- Be aware that child-on-child abuse can happen online.
- Report all concerns about child-on-child abuse to the DSL immediately.
- Understand that victims should never be blamed and must be supported.
- Follow the school's child protection policy when dealing with incidents.
- Teach pupils about respectful relationships online.
- Create a culture where pupils feel safe to report concerns.

Accessibility and Inclusion

CLPT is committed to ensuring that ICT systems and practices are accessible and inclusive for all staff and pupils, including those with SEND. We will:

- Ensure ICT equipment and software is accessible to staff and pupils with disabilities.
- Make reasonable adjustments to ICT systems and practices where required under the Equality Act 2010.
- Provide appropriate assistive technology for staff and pupils who need it.
- Ensure online safety teaching is accessible and appropriate for all pupils, including those with SEND.
- Monitor ICT use to ensure no group is disadvantaged or discriminated against.
- Provide training and support for staff on making ICT accessible.
- Work with pupils, parents and specialists to identify and meet individual needs.

Asset Register

We hold an information asset register in school that is stored on the trust's network (restricted access). This document is under continual review due to the nature of the information contained within it. The register includes:

- All ICT equipment owned by the school
- Software licences
- Data assets and their classifications
- Who is responsible for each asset

- Location of assets
- Review dates

Personal Network Storage/Cloud Storage

- Items that are stored and saved on the school network are owned by the school - they should not be removed without permission.
- Staff must save documents on the school network in a structure agreed by the Headteacher/DHT.
- Staff should not create folders in the shared areas unless approved by the Headteacher/DHT.
- Shared areas should only be used for documents and resources that you wish to share with others.
- Personal documents should be stored in your 'My Documents' area or OneDrive.
- Staff must ensure that these areas stay free from clutter.
- When pupils leave school, it is the responsibility of class teachers to delete any electronic records relating to these pupils in line with the school's retention schedule. Paper copies will have gone with the pupil to the new school.
- Staff should aim to minimise the items on their desktop in favour of shared areas or their home drive.

Microsoft 365

The Trust is moving towards a cloud centric network, with Microsoft 365 at the core. Staff may use this area to store or share documents with authorised people. This area is shared only with the school community. Passwords must not be written down or shared. Staff must:

- Only share documents with appropriate colleagues.
- Ensure appropriate permissions are set on shared documents.
- Not share confidential information inappropriately.
- Report any security concerns immediately.

Clear Desk Policy

CLPT operates a clear desk policy whereby confidential papers are NOT left lying on desks. Lockable filing cabinets/drawers should be used and keys removed from the locks and stored in a safe place. This includes:

- Locking away all confidential documents at the end of each day.
- Not leaving sensitive information visible on screens.
- Logging off or locking computers when leaving desks.

- Securing keys appropriately.

Process for Allowing Third Parties Access to School Systems

We will allow third parties access to our systems, for example to provide remote IT support or premises users such as the school nursing team access to the guest Wi-Fi. Access is granted by the Headteacher and CLPT IT Department on a case-by-case basis and assurances are sought as to the need to comply with data protection and security legislation.

Third parties must:

- Sign an acceptable use agreement before being granted access.
- Only access systems for the agreed purpose.
- Comply with all school policies relating to data protection and ICT security.
- Report any security concerns immediately.
- Not share access credentials with others.

Access will be reviewed regularly and revoked when no longer required.

Physical Security

The building is protected by an alarm system. During opening hours, staff (includes CPMS staff, Physios, School nurse etc.) gain entry via a swipe system. Key areas containing information are secured by keypads e.g. Main office, Headteacher's office, DHT's office, Staffroom and photocopier room.

All visitors must report to reception. Credentials are checked and any visitors must sign in/out and will be issued with a visitor's badge (this will be on a lanyard that will clearly display their role e.g. Trustee, Governor, parent, visitor, volunteer, student, contractor etc.). Mobile phones are to be handed in to reception where they will be stored securely in a locked drawer or left in owners' vehicles.

All internal and external gates/doors to be refastened/closed after passing through. Windows and doors are to be closed and locked when rooms left vacant. The office window will be shut and locked when the office is unattended.

Only authorised personnel have access to keys to the building and they must sign a declaration form accepting responsibility when these are given. Keys will only be given to contractors as a last resort and information will be secured during these times. Any contractors requiring keys must sign a declaration.

Access is restricted to authorized personnel for keys to data stored in secure areas.

(See Security - Entry & Exit Procedures and key holders and code holders policy)

Training

All school personnel:

- have equal chances of training, career development and promotion;

- receive training on this policy on induction which specifically covers:
    - Computer Misuse
    - Data Protection and UK GDPR
    - Copyright
    - Equal opportunities
    - Inclusion
    - Online safety (including understanding of filtering and monitoring systems)
    - Safeguarding (including child-on-child abuse online)
    - Low-level concerns
- receive online safety and child protection training (including understanding of filtering and monitoring systems) at induction and at least annually through updates (e.g. via email, e-bulletins, staff meetings);
- receive periodic training so that they are kept up to date with new information;
- receive equal opportunities training on induction in order to improve their understanding of the Equality Act 2010 and its implications.

The DSL and deputies will receive additional specialist training as required by Keeping Children Safe in Education 2025.

Acceptable Use Declarations

CLPT expects all school personnel to sign and date the 'Acceptable Use of ICT Agreement' to confirm they have read and understood their obligations. They must also be fully aware of and implement any linked policies (see list of linked policies). All school personnel have the duty to report any misuse of ICT equipment or ICT facilities to the DSL or Headteacher/Deputy Headteacher.

Visitors to the school are not permitted to use the school network or any school devices without signing the relevant acceptable use agreements.

The trust reserves the right to refuse access to the network at any time.

Acceptable User Guidelines For School Network Users

- All of the school ICT resources (Internet, portable devices, switches and communication devices etc.) are to be used for educational purposes only.
- It is the personal responsibility of all staff to abide by the set rules and regulations when using any of the school's ICT resources and to understand that there may be consequences if they breach them.
- All accidental access to inappropriate material or websites should be reported immediately to the DSL or Headteacher/DHT.

- Staff will log on to the computer/internet by using a password, which will be changed every 3 months, or more often if there is a potential security breach.

IT Users must not:

- use the Internet in such a way that will bring the school into disrepute;
- use inappropriate or illegal websites;
- download inappropriate material or unapproved software;
- disrupt the time of other Internet users by misusing the Internet;
- use inappropriate language;
- use language that may provoke hatred against any ethnic, religious or other minority group;
- produce, send out, exhibit or publish material that will cause offence to anyone;
- divulge any personal information about themselves or any other user or that of pupils;
- divulge personal login credentials or passwords to anyone;
- use the login credentials or passwords of any other user;
- use a computer that is logged on by another user;
- use any social networking site for communication with pupils or parents of the school;
- use images of pupils without prior permission of the Headteacher and parents;
- use CLPT/School email for private use. It should only be used for educational purposes;
- compromise the Data Protection Act 2018, UK GDPR or the law of copyright in any way;
- engage with or promote harmful online challenges or hoaxes;
- engage in any form of child-on-child abuse online;
- use unauthorised AI tools or generative AI applications.

Electronic Data Protection and Data Storage

- Data is any information that is considered to be personal, sensitive or valuable to individuals or the school.
- Data relating to work should be stored on the school network (see Network Storage).
- The use of removable media (USB pen drives, CDs, portable drives) is prohibited in school unless permission has been granted by the CLPT IT Department.
- Data stored on loaned devices should be encrypted.
- Data pertaining to the school should never be stored on personal devices.
- Data should only be removed from school if you have been authorised to do so.

- If approved, data should only be taken when it is required to fulfil your role. If you are unsure speak to the Headteacher/DHT.
- Data in your possession becomes your responsibility - you must keep it secure and in your possession at all times.
- You must not carry all your data with you all the time. Data in your possession should be adequate, relevant and not excessive (The Data Protection Act 2018 and UK GDPR). (Complete the task, return the data)
- If you have been authorised to take data to fulfil your role but do not own a school device, the information should be stored using Microsoft OneDrive through Launchpad 365. If you are unsure speak to the Headteacher/DHT.
- When completing data at home (PLPs, assessment records) staff must remove sensitive information. For instance, complete the document using initials instead of full names. Remove dates of birth, phone numbers, email addresses and other personal information that connects the document to an individual or associates. These fields can be filled out once the document returns to school.
- Photos (paper format) are taken out of school in exceptional circumstances with safeguards in place.
- Any loss of data should be reported immediately to the Headteacher/DHT for escalation. Staff must ensure that they are aware of any linked policies to data protection and data storage.
- When photos are used e.g. in the calendar, explicit consent has been sought.
- Data must be retained only for as long as necessary in accordance with the school's retention schedule.
- Data must be disposed of securely when no longer required (e.g. shredding, secure deletion).
- These guidelines are designed to inform and protect CLPT and its associates from online safety incidents and promote a safe e-learning environment for pupils. Failure to follow these guidelines will be treated seriously and could lead to disciplinary procedure.

Relevant Legislation

- This should be read in conjunction with:
- Keeping Children Safe in Education (2025)
- Computer Misuse Act 1990
- Data Protection Act 2018
- UK General Data Protection Regulation (UK GDPR)
- Human Rights Act 1998

- Freedom of Information Act 2000
- Equality Act 2010
- Health and Safety (Display Screen Equipment) Regulations 1992
- The Education Act 2002
- The Children Act 1989

The following documentation is also related to this policy:

- Data Protection and Security: A Summary for Schools (Becta 2004)

Linked Policies

- Safeguarding Policy (including Child Protection)
- Staff Code of Conduct
- Data Protection Policy
- Online Safety Policy
- Behaviour Policy
- Mobile Phone Policy
- Safer Recruitment Policy
- Low-Level Concerns Policy
- Relationships and Sex Education Policy
- Equality and Diversity Policy
- Staff Disciplinary Policy
- Whistleblowing Policy

Policy Review

- This policy will be reviewed annually (as a minimum) and updated as needed to reflect:
- Changes in legislation (particularly KCSIE updates)
- Changes in technology
- Emerging online safety threats
- Lessons learned from incidents
- Feedback from staff, pupils and parents
- Changes in school procedures or structure
- The next review date is: **Autumn Term 2026**

Acceptable ICT Use Agreement

I understand that all of the school ICT resources (Internet, portable devices, switches and communication devices etc.) are for the good of my professional development and the development of this school. They must be used only for educational purposes.

I realise that it is my personal responsibility to abide by the set rules and regulations when using any of the school's ICT resources and am aware of the consequences if I breach them. This relates to this policy and all linked policies.

I will report immediately to the DSL or Headteacher/DHT any accidental access to inappropriate material or websites that I or others may have made.

I will log on to the Internet by using my password, which will be changed every 3 months, or if I think someone knows it.

In addition I will not:

- use the Internet in such a way that it will bring the school into disrepute;
- use inappropriate or illegal websites;
- download inappropriate material or unapproved software;
- disrupt the time of other Internet users by misusing the Internet;
- use inappropriate language;
- use language that may provoke hatred against any ethnic, religious or other minority group;
- produce, send out, exhibit or publish material that will cause offence to anyone;
- divulge any personal information about myself, any other user or that of pupils;
- divulge my login credentials or passwords to anyone;
- use the login credentials or passwords of any other user;
- use a computer that is logged on by another user;
- use any social networking site for communication with pupils or parents of the school;
- use images of pupils without prior permission of the Headteacher and parents;
- use email for private use but only for educational purposes;
- compromise the Data Protection Act 2018, UK GDPR or the law of copyright in any way;
- engage with or promote harmful online challenges or hoaxes;
- engage in any form of child-on-child abuse online;
- use unauthorised AI tools or generative AI applications.

I understand that:

- All internet use is filtered and monitored;
- I have a responsibility to report online safety concerns to the DSL;
- I must understand how filtering and monitoring systems work;
- Low-level concerns about ICT use will be recorded and may lead to further action;
- Child-on-child abuse can occur online and I must be vigilant;
- I must ensure ICT systems and practices are accessible and inclusive for all.

I have read and understood:

- The Information Security and Acceptable Use Policy
- The Safeguarding Policy (including Child Protection)
- The Staff Code of Conduct
- The Online Safety Policy
- My responsibilities in relation to filtering and monitoring systems

I agree to abide by the Acceptable Use Policy.

Employee Name:		**Headteacher Name:**	
Employee Signature:		Headteacher Signature:	
Date:		Date:	

ICT Concern / Misuse Form

All security breaches (loss of equipment or data, unauthorised or misuse of ICT, theft of equipment or data, online safety concerns) should be reported immediately to the DSL or Headteacher/DHT for escalation.

Person Reporting Incident:

Name:

Role:

Date and Time of Incident:

Type of Incident: (please tick)

☐ Loss of equipment
☐ Loss of data
☐ Theft of equipment
☐ Theft of data
☐ Unauthorised access
☐ Misuse of ICT
☐ Online safety concern
☐ Child-on-child abuse online
☐ Harmful online challenge/hoax
☐ Breach of acceptable use policy
☐ Low-level concern
☐ Filtering/monitoring system failure
☐ Other (please specify): _____

What happened? (Please provide as much detail as possible)

Location of incident:

Were any pupils involved? ☐ Yes ☐ No

If yes, please provide details (names, year groups):

Were any other staff members involved? ☐ Yes ☐ No

If yes, please provide details:

Has this been reported to anyone else? ☐ Yes ☐ No

If yes, who:

Immediate action taken:

Data Affected

Type of data involved: (please tick all that apply)

☐ Pupil personal data
☐ Staff personal data
☐ Parent/carer data

☐ Sensitive/confidential data
☐ Financial data
☐ No data involved
☐ Other (please specify): _____

Number of individuals affected:

Has this been reported to the DPO? ☐ Yes ☐ No ☐ N/A

Signed (user): _____ Date: _____

To be completed by DSL/Senior Leadership Team:

Date received:

Received by:

Initial assessment:

☐ Safeguarding concern - refer to safeguarding procedures
☐ Low-level concern - record and monitor
☐ Data breach - report to DPO
☐ Disciplinary matter
☐ Training need identified
☐ Policy review needed
☐ Other: _____

Action to be taken:

Has this been reported to:

☐ Headteacher
☐ DSL
☐ DPO
☐ Governors
☐ Police
☐ Local Authority
☐ ICO (if data breach)
☐ Parents
☐ Other: _____

Follow-up actions required:

Review date:

Signed (Senior Leadership): _____ Date: _____

Summary of Key Changes Made

- Updated KCSIE reference to 2025 version throughout
- Designated Safeguarding Lead (DSL) role clearly defined with specific responsibilities
- Filtering and monitoring systems section with detailed explanation of how systems work and staff responsibilities
- Low-level concerns section with clear definition, reporting procedures and recording requirements
- Annual training requirement explicitly stated for online safety and safeguarding
- Child-on-child abuse online section with examples and reporting procedures
- Harmful online challenges and hoaxes section
- AI and Generative AI section with guidance on appropriate use
- Accessibility and inclusion section addressing Equality Act 2010 requirements
- Enhanced data protection references to Data Protection Act 2018 and UK GDPR
- Updated acceptable use agreement reflecting all new requirements
- Enhanced incident reporting form with specific categories for new concerns
- Review date updated to Autumn Term 2026 with commitment to annual review
- Strengthened references to linked policies including safeguarding and child protection