Information Security and Acceptable Use Policy

Approved by:	Chair of Trustees Chief Executive Officer	Date: Summer Term 2023
Next review due by:	Summer Term 2025	

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 this school. 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 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 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) adhere 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. 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) provides 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 Entrust).
- 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;
- make 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 Entrust);
- Liaise with Entrust to provide staff with correct software (encryption, antivirus, firewall etc.)
- keep up to date with new developments and resources;
- undertake risk assessments when required;

Maintaining the security of the school's IT Network

The Director of Operations, working with Headteachers, are responsible with the aid of Entrust for maintaining the school network. The Director of Operations, working with Headteachers must ensure that virus protection is up to date, 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 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;
- 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.

Overview

- Staff should receive regular updates and training through weekly meetings and inhouse training
- Staff must make themselves familiar with all school policies and linked policies relating.
- New staff should receive relevant policies as part of their induction.
- Staff must understand their roles and responsibilities in online safety.
- Staff must report misuse of the school network and equipment immediately
- Staff must report theft, loss or damage to/of data or equipment immediately
- 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 to how to report abuse by speaking to any member of staff (who will escalate the concern to the 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. provides a comprehensive online safety education programme for pupils, staff and parents, as appropriate.

Monitoring of IT systems

- The Head Teacher or IT lead 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, or to prevent or detect crime.

- Securus Software 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

Security Incident / Breach reporting

Concerns

Everyone connected with their school is encouraged to report online safety concerns immediately to the Headteacher / DHT for escalation.

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).
- 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

Internet Use

All schools in The Creative Learning Partnership Trust use broadband provided through Entrust. 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 and the relevant documentation have 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. Arrangement 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.

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*
Business (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. (CTRL+ALT+ DELETE 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 fulfill 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 or USB with 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.

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. (CTRL+ALT+ DELETE 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.
    - 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 or 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.

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.

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 Headteacher / DHT.
- Staff should ensure that when a device require updates, these are implemented. Do not ignore the requests.

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.
- When photos are used e.g. in the calendar, explicit consent has been sought

Protective marking

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

Public	*No need to mark public documents*
Business (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 the external sources.

Backups

Data is backed up to the school server and to the cloud every 4 hours.

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)

Asset register

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

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 Teachers.
- 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
- 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. Paper copies will have gone with the pupil to the new school.
- Staff should aim to minise the items on their desktop in favour of shared areas or their home drive.

Office 365

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.

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.

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 Wifi. Access is granted by the headteacher on a case by case basis and assurances are sought as to the need to comply with data protection and security legislation.

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
    - Copyright
    - Equal opportunities
    - Inclusion

- 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

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 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 school 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 schools ICT resources and to understand that there may be consequences if these are breached them.
- All accidental access to inappropriate material or websites should be reported immediately to the Headteacher / DHT.
- Staff will log on to the computer / internet by using a password, which will be changed every half term, 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 associates of any schools
    - 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 or the law of copyright in any way

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 Headteacher
- 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, and relevant and not excessive (The Data Protection Act 2018). (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 (PLP's, assessment records) staff must remove sensitive information. For instance complete the document using initials instead of full names. Remove dates of births, 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.

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 (2022)*
- Computer Misuse Act 1990
- Misuse of Information Act 1990
- Health and Safety (Display Screen Equipment) Regulations 1992
- Data Protection Act 2018
- Human Rights Act 1998
- Freedom of Information Act 2000

The following documentation is also related to this policy:

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

Linked Policies

Safeguarding Policy
Staff code of conduct
Data protection
Online Safety
Behaviour Policy
Mobile Phone Policy

Appendix 1:

Acceptable ICT Use Agreement

I understand that the 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 schools 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 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 half term, 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 associates of any schools
- 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 or the law of copyright in any way

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) should be reported immediately to the Headteacher / DHT for escalation.

Person reporting incident:

Name: **Role:**

What happened?

Data effected

Signed (user) _____ **Date:**_____

To be completed by member of leadership team:

Action to be taken

Signed (Senior leadership) _____ **Date:**_____