ICT Acceptable Use Policy

A Trust-wide policy for all Chiltern Learning Trust schools

Date Approved	**Body**	**Next Review Date**
[Insert date]	Board of Trustees	
Author	**Owning Department**	
Head of Operations	Central Operations	

This policy applies to all Chiltern Learning Trust schools and the Central Team.

Contents

1. Introduction and Scope
2. Definitions
3. Roles and Responsibilities
4. Acceptable Use of ICT Facilities
5. Email, Telephone and Devices
6. Personal Use of ICT Facilities
7. Social Media
8. Images of Pupils, Staff and the School Community
9. Artificial Intelligence
10. Data Security and Cyber Security
11. Filtering and Monitoring
12. Internet Access
13. Monitoring and Review of this Policy
14. Related Policies, Legislation and Guidance

Appendix 1: Acceptable Use Agreement – Staff, Governors, Volunteers and Contractors

Appendix 2: School-Specific Information

Appendix 3: Device Loan Agreement

1. Introduction and Scope

Information and communications technology (ICT) and social media are integral to how Chiltern Learning Trust and its schools operate. They support teaching and learning, communication with families and the day-to-day running of our schools.

This compulsory policy sets out what the acceptable usage requirements are for everyone who uses Trust ICT facilities.

This policy applies to all users of our ICT facilities and social media including:

- Staff
- Trustees
- Governors
- Volunteers
- Contractors
- Visitors

Breaches of this policy may be dealt with under the Trust's Code of Conduct or, for pupils, the school's Behaviour Policy.

This policy works alongside other Trust policies, each of which covers its own area in full detail.

Topic	**Where to find full detail**
Artificial Intelligence (AI) tools and generative chatbots	Artificial Intelligence Policy
Cyber security controls, passwords, Multi Factor Authentication (MFA), Bring Your Own Device (BYOD)	Cyber Security Protocol
Images and videos of pupils, staff or visitors	Using Images Safely in CLT Schools guidance
Safeguarding, online safety, filtering and monitoring roles	Safeguarding Policy (including Appendix 7)
Personal data, subject access requests, data breaches and FOI requests	Data Protection Policy

3. Definitions

Term	**Definition**
ICT facilities	All Trust and school network infrastructure, devices, software, websites, web applications and licensed hosted services, including anything provided for the Central Team.
Users	Anyone authorised to use ICT facilities, including staff, governors, trustees, volunteers, contractors and visitors.

Materials	Any files or data created using our ICT facilities, including documents, photos, audio, video, printed output, web pages, social media content and resources created/used under licence with applicable copyright .
Social media	Any online platform or application that allows people to communicate instantly or share content publicly, including networking sites, blogs, video and image-sharing sites,platforms and messaging apps.
Personal use	Any use of ICT facilities that is not directly related to a user's employment, study, or an agreed purpose.
Authorised personnel	Staff authorised by the school or Trust to administer or monitor ICT facilities.

4. Roles and Responsibilities

Board of Trustees

Approves this policy and is accountable for making sure the Trust meets the DfE's filtering and monitoring standards and cyber security expectations.

ICT Operations Manager

Updates and owns the Policy

Headteacher and Senior Leadership Team

Make sure staff understand and follow this policy and act on any concerns or reports raised.

Designated Safeguarding Lead (DSL)

Takes lead responsibility for understanding the filtering and monitoring systems in place and for any safeguarding concern that arises through them. Full detail is set out in the Safeguarding Policy.

Trust EdTech Lead

Supports schools with the safe adoption of AI and other education technology and maintains the Approved AI Tool Register.

IT Service Provider

Maintains the technical infrastructure, filtering and monitoring systems, and responds to reported incidents. Full detail is set out in the Cyber Security Protocol.

All users

Everyone who uses our ICT facilities is responsible for using them in line with this policy and for reporting concerns promptly.

5. Acceptable Use of ICT Facilities

5.1 General Principles

Staff will be provided with unique login details and passwords and are required to set-up Multi Factor Authentication (mfa) which must be kept secure and never disclosed. Access permissions are managed by the Trust IT Provider with the permissions guided by the Head of Operations.

Parents and carers do not have access to Trust ICT facilities, unless working with the school in an official capacity (for example, as a volunteer) and any such access must follow this policy in full.

5.2 Unacceptable Use

The following is considered unacceptable use of the Trust's or a school's ICT facilities. Any breach may result in disciplinary or behaviour proceedings. This list is not exhaustive.

- Breaching intellectual property rights or copyright
- Bullying, harassment, or promoting unlawful discrimination
- Any illegal conduct, or content advocating illegal activity
- Online gambling, inappropriate advertising, phishing or financial scams
- Accessing, creating, storing or sharing material that is pornographic, offensive, obscene or otherwise harmful
- Consensual or non-consensual sharing of nude or semi-nude images, videos or livestreams
- Activity that defames or disparages the Trust or a school, or risks bringing either into disrepute
- Providing, sharing or allowing access to confidential information about the Trust, a school, pupils, or members of the school community
- Connecting any device to the school network without authorisation
- Installing software or applications, or using any tool designed to interfere with the school's ICT facilities, without authorisation
- Gaining, or attempting to gain, unauthorised access to systems, accounts or password-protected information
- Causing intentional damage to ICT facilities, or removing or disposing of equipment without permission
- Causing a data breach by accessing, modifying or sharing data without authorisation
- Using inappropriate or offensive language
- Promoting a private business unrelated to the Trust or school
- Bypassing or attempting to bypass the school's filtering or monitoring systems
- Content or conduct that is radicalised, extremist, racist, antisemitic or otherwise discriminatory
- Using AI tools or generative chatbots that are not on the Trust's Approved AI Tool Register (see section 10)

6. Email, Telephone and Devices

Staff must use their school-issued email address for all work-related business and enable multi-factor authentication. Personal (non-work) email addresses must never be used to send work-related materials, and staff must not disclose their personal email address with parents, carers or pupils.

Staff must take care with the content of emails, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation or breach of confidentiality. Emails may need to be disclosed in legal proceedings or in response to a subject access request, even after deletion from an inbox.

Staff must not give their personal phone number to parents, carers or pupils, and must use school-provided phones or numbers for all work-related business.

Staff personal devices must not be connected to the Trust Wi-Fi or used for school related work.

Guest Wi-Fi is offered on a case by case basis, is managed by the Headteacher (nominated admin), is monitored and passwords updated weekly.

Staff will be provided access to a school owned device to complete their role. If this is a mobile device, chromebook, laptop etc) a Device Loan Agreement form must be signed on receipt and handed to HR - Appendix 3

Note: some schools record incoming and outgoing calls. Callers are notified. Any request to record a conversation outside of this must be pre-approved and with consent from all parties.

> *Full detail on remote access, personal devices and technical security controls is set out in the Cyber Security Protocol.*

7. Personal Use of ICT Facilities

Staff may occasionally use school ICT facilities for personal use. This is a privilege, not a right, and may be withdrawn at the school's discretion. Personal use is only permitted where it:

- Takes place outside working time, in a break
- Does not constitute unacceptable use, as set out in section 5.2
- Takes place when no pupils are present
- Does not interfere with anyone's job, or prevent others from using the facilities for work or educational purposes

Staff must not use school ICT facilities to store personal, non-work-related material such as music, videos or photos. Personal use may fall within the scope of the school's monitoring activity described in section 11.

8. Social Media

There are two types of communication covered by this policy: personal communications, made on a personal social media account, and professional communications, made through official Trust or school channels.

Professional communications must always follow the Trust's and school's guidance for official accounts. Only staff authorised to manage an official account may post to it.

Personal communications are permitted but if a conversation becomes public and its content is inappropriate or unprofessional, disciplinary action may be taken. Staff should ask themselves: “If this became public knowledge, could it raise questions about my suitability to work in a school or Trust, or bring the school or Trust into disrepute?”

Staff must not:

- Disclose private or confidential information about pupils, parents, colleagues, or the Trust, including in relation to any previous educational employer
- Identify themselves as a representative of the school or Trust on a personal profile

- Post abusive comments about current or former colleagues, pupils or parents
- Access personal social media accounts during the working day, other than during a designated break
- Post images of pupils, or of colleagues (without their permission), from this or any previous school
- Set up or use an alias account to get around this policy
- Use social media to raise or escalate a concern about the school or Trust — concerns should go through a line manager, the Grievance Procedure or the Whistleblowing Procedure

> *Full guidance on managing privacy settings the 12 rules for personal use of social media is outlined in the Using Images Safely in School Guidance*

9. Images of Pupils, Staff and the School Community

Every school and staff member must follow the Trust's Using Images Safely in CLT Schools guidance, alongside the UK Safer Internet Centre's guidance on Protecting your Settings Images from AI manipulation and abuse.

This includes, in summary: using only school-owned devices to capture images, avoiding identifiable faces on publicly accessible platforms, gaining annual informed consent, storing images securely, and removing images promptly when a pupil leaves the school.

> *Staff, volunteers and contractors must read and follow the Using Images Safely in CLT Schools Policy in full before capturing or sharing any image of a pupil or member of staff.*

10. Artificial Intelligence

Only AI tools on the Trust Approved AI Tool Register may be used by staff or pupils. Any new tool must be reviewed by the Trust EdTech Lead against the DfE's product safety expectations, and a Data Protection Impact Assessment (DPIA) must be completed and approved by the Headteacher/Directors as outlined in the GDPR Policy.

Staff must never input personal or sensitive pupil data, or pupil work into an AI system that is not on the Trust Approved AI Tool Register. This risks a data protection breach or a breach of intellectual property.

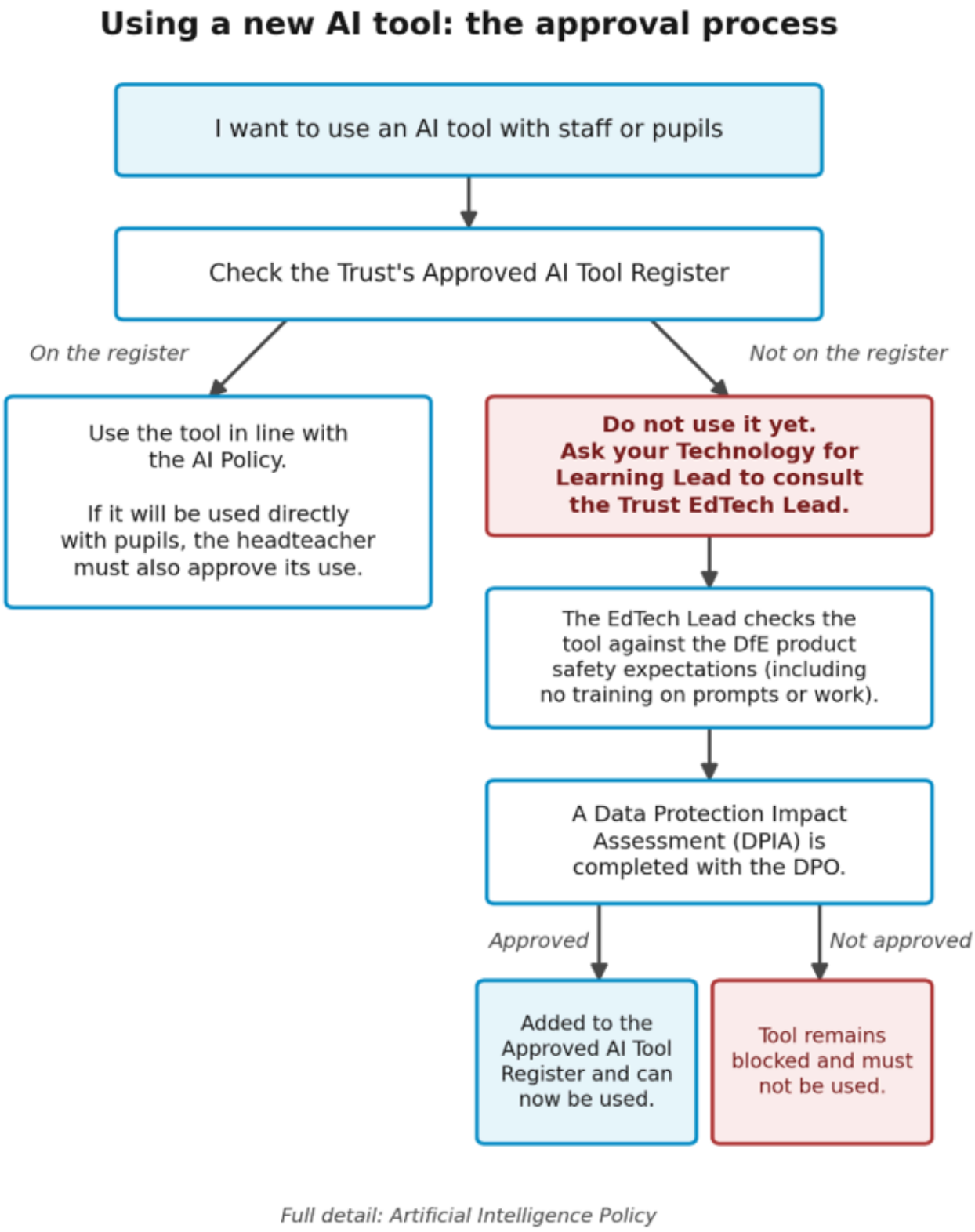


Figure 1: the approval process for a new AI tool. Full detail is set out in the Artificial Intelligence Policy.

11. Data Security and Cyber Security

The Trust takes steps to protect its systems, data and users, including firewalls, anti-malware software, and multi-factor authentication. All users must set strong, unique passwords, keep them secure, and never share or disclose account details. Devices and systems must be logged out and locked when not in use.

If you notice anything that could be a cyber or data security incident for example a suspicious email, a lost device, information sent to the wrong person or a ransomware demand immediately report this to your school IT contact and your line manager.

> *Full details on remote access Cyber Security requirements are set out in the Cyber Security Protocol and on the approval process for software in the Data Protection Policy .*

12. Filtering and Monitoring

To safeguard pupils and provide a safe environment to learn, the Trust filters and monitors the use of its ICT facilities and network, including internet sites visited, email accounts and user activity. Only authorised School and ICT personnel may access this information.

Monitoring is carried out to keep pupils safe, investigate compliance with school policies, ensure effective ICT operation and to comply with legal obligations such as a subject access request.

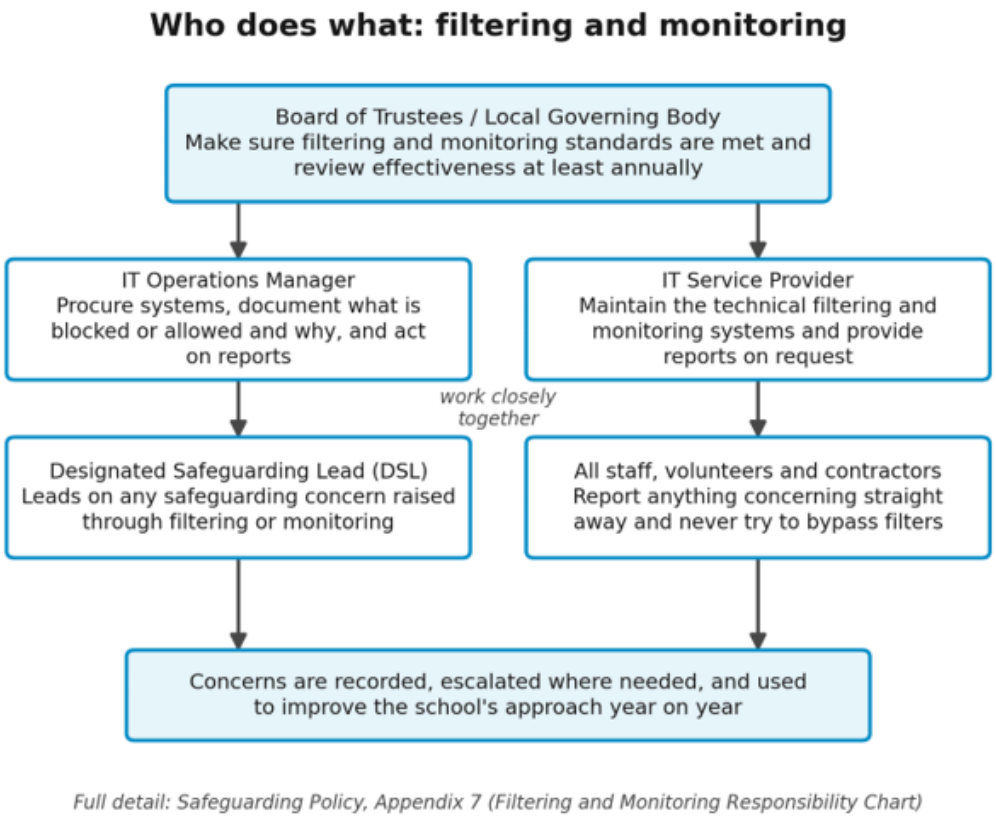


Figure 3: who is responsible for what. The full Filtering and Monitoring Responsibility Chart is set out in the Safeguarding Policy, Appendix 7.

13. Internet/Wifi Access (wifi network access including but not limited to access to the internet).

Visitors may not use the school's Wi-Fi/Internet unless this has been set-up and specifically authorised; for example for an event. In this instance a specific password will be generated and then cancelled once the event is completed.

14. Monitoring and Review of this Policy

The headteacher, IT Operations Manager and the Trust ICT provider are responsible for the day-to-day implementation of this policy. This policy is reviewed annually and approved by the Board of Trustees.

15. Related Policies

This policy should be read alongside:

- Artificial Intelligence Policy
- Cyber Security Protocol
- Data Protection Policy
- Safeguarding Policy
- Using Images Safely in CLT Schools guidance
- Behaviour Policy
- Staff Code of Conduct
- Mobile Phone Policy

Legislation and Guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR)
- The Data (Use and Access) Act 2025
- Computer Misuse Act 1990
- Human Rights Act 1998
- Education Act 2011 and Education and Inspections Act 2006
- Freedom of Information Act 2000
- Keeping Children Safe in Education (KCSIE)
- DfE guidance: Meeting digital and technology standards in schools and colleges (including the filtering and monitoring standards)
- DfE guidance: searching, screening and confiscation
- DfE guidance: political impartiality in schools
- DfE's product safety expectations for AI tools in education
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- UK Council for Internet Safety guidance on sharing nudes and semi-nudes

Appendix 1 : Acceptable Use Agreement — Staff, Governors, Volunteers and Contractors

By reading and acknowledging this policy on Policy Viewer staff confirm that they have read and understood the ICT Acceptable Use Policy and agree to comply with it. I understand that:

- My use of the Trust's ICT facilities may be monitored, as set out in section 12
- Any breach of this policy may be dealt with under the Trust's Code of Conduct and may result in disciplinary action
- I must report any concern about a possible cyber or data security incident to my school's IT contact and my line manager immediately
- I must use only AI tools on the Trust's Approved AI Tool Register
- I must include the DPL/DPO in any process of considering new software as noted in the Data Protection Policy and any additional guidance outlined in this policy.

Appendix 2: School-Specific Information

Every school must complete this page

School Name / Central Team	
Headteacher	
School ICT / network contact	Redsquid Education
Designated Safeguarding Lead (DSL)	
Data Protection Lead (DPL)	
Wi-Fi authorisation contact (for visitors)	
Any other school-specific ICT policies	

Appendix 3: Device Loan Agreement Form

Device Loan Agreement (Staff)

1. This agreement is between:

I. Chiltern Learning Trust “the employer”
II. Employee:

It governs the use and care of devices assigned to individual staff members. This agreement covers the period from the date the device is issued through to the return date of the device to the school/Trust.

All issued equipment shall remain the sole property of the school/Trust and is governed by the school’s/Trust’s policies as detailed below.

a) The school/Trust is lending the employee the following device:

Make & Model: _____

Serial Number: _____

b) This agreement sets the conditions for the employee using the device.

I confirm that I have read the terms and conditions set out in the agreement and my signature at the end of this agreement confirms that I have read and agree to all these terms.

2. Damage/Loss

I understand that I am responsible for the equipment at all times whether on any Trust sites or not. If the equipment is damaged, lost or stolen, I will immediately inform my line manager and HR. Whilst the device is offsite, I acknowledge that I am responsible for the full replacement costs if the equipment is damaged or misused. If the equipment is stolen, I will also immediately inform the police.

I agree to keep the equipment in good condition and to return it to the school/Trust on demand.

I will not leave the equipment unsupervised in unsecured areas.

3. Unacceptable use

I am aware that the school/Trust monitors my activity on the equipment.

I will not carry out any activity that constitutes ‘unacceptable use’.

I can confirm that I have read the Trusts ICT & Internet Acceptable Use Policy and Cyber Security Protocol and understand that this must be adhered to at all times.

I accept that if I engage in any activity that constitutes ‘unacceptable use’, I may face disciplinary action in line with the Trusts Code of Conduct..

4. Data protection

All of the Trust's and School's ICT devices that support software updates, security updates and anti-virus products will have these installed and be configured to perform such updates regularly or automatically.

Staff are required to :

- Keep the equipment password-protected in line with school/Trust policy -
- Lock the device when not in use and have autolock activated as an additional precaution
- Do not share or loan the equipment among family or friends
- Install the latest updates to operating systems, as prompted

If staff require IT support; please raise a support ticket directly with the Trust IT Support Provider.

5. Return Date

Staff will return the device in an acceptable condition within 5 days of being requested to do so or with immediate effect if requested by HR.

Staff will return the equipment to the school/Trust on my last working day of employment whether that be due to my resignation, dismissal or if I leave the employment of the school/Trust for any other reason.

6. Consent

By signing this form, the employee confirms that they have read and agree to the rules and conditions above.

FULL NAME	
SIGNATURE	

……

Associated Documents & Roles	
Document Name	**Description**
Data Protection Policy	Outlines how data management and protection is conducted
Keeping Children Safe in Education Policy	Outlines safeguarding practices
Cyber Security Protocol	Outlines cyber best practices and staff responsibilities
Acceptable Use Policy	Outlines acceptable use of technology in school

Trust AI Policy	This AI policy outlines the guidelines and measures that all schools and staff within the Trust must follow to establish a consistent approach to AI.