ICT and AI Acceptable Use Policy

Document Control	
Document Title:	ICT and AI Acceptable Use Policy
Version:	1
Summary of Changes from Previous Version:	Inclusion of section '3.15' which covers guidance on the use of AI.
Name of Originator/Author (including job title):	Lauren Thorpe, Chief Transformation Officer
Target Audience:	All staff
Review By Date:	September 2026
Date Issued:	September 2025

Contents

Contents

1. Scope

1.1 The policy and procedure set out in this document applies to all Trustees and LGB members, and to all staff employed by United Church Schools Trust (“UCST”) and United Learning Trust (“ULT”) including teaching, non-teaching, fixed term, part-time, full-time, permanent and temporary staff.

1.2 This policy has been updated to include safeguards to ensure the acceptable use of AI.

1.3 As a values-led organisation, our values of ambition, confidence, creativity, respect, enthusiasm and determination are key to our purpose and underpin all that we do.

2. Implementation

2.1 Schools must ensure continuous compliance with this policy and comply with all related policies.

3. Policy Acceptance

All employees must read and confirm that they agree to abide by this Acceptable Use Policy before they can be allowed to use devices or services provided by or on behalf of United Learning. All employees will be required to review and confirm their ongoing acceptance of this policy via an annual renewal form.

By completing the relevant section of the Annual Renewal form you agree to the following:

3.1 An authorised representative of the Group may view, with just reason and without notice or notification, any communications you send or receive, material you store on the Group’s computers/ services or logs of websites you have visited. This data, regardless of where hosted, belongs to United Learning at all times. It is the Group’s policy not to view colleagues’ emails without good cause.

3.2 You will only access those services/ aspects of services which you have been given permission to use.

3.3 You will not use United Learning resources (including, but not limited to, equipment and software) to operate your own business.

3.4 You will not attempt to remove any of the security measures put in place by United Learning to ensure the integrity of its services, the security of its data or the appropriateness of employee activity.

3.4.1 If a machine is not routinely connected to the school network, provision must be made for regular virus updates.

3.4.2 If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact the ICT department. They will advise you what actions to take and be responsible for advising others that need to know.

3.5 Any communication from a United Learning related account (email, social media) or account which identifies you as belonging to United Learning will be appropriate in tone and content.

3.6 You will exercise caution when sending information via email to ensure that it is addressed to the correct recipient(s) and is the correct information (particularly when attaching documents). Personal data (that by which an individual could be identified) must not be transferred to other recipients unless encrypted or password protected, in line with the requirements of Data Protection legislation.

3.7 You will not transfer United Learning data outside of the organisation's systems except via Group email or encrypted media. This includes the use of cloud storage and personal email accounts. For example, saving files to Dropbox or emailing them to a personal Hotmail account may resolve logistical problems you are having but run the risk of those data leaving United Learning's control.

3.8 You will not use non-United Learning systems to carry out any work-related activities, or communications about work, which contain personal or identifiable information about staff or pupils.* For example, using a WhatsApp group to discuss HR issues or pupil behaviour.

3.9 You will not use non-United Learning systems to communicate with pupils, prospective pupils or their parents about school-related activities, in line with the annual staff-student relationship letter.

3.10 You will use the Internet and other services for appropriate activity only. United Learning considers inappropriate activities to include (but not limited to) gambling (outside of workplace Lottery syndicates), pornography, accessing the dark web, and sites promoting views which run counter to the organisation's ethos.

3.11 You will not share your access credentials with anyone. Delegated access to calendars/ email should be granted to administrative support staff, where required.

3.12 You will not download, use, distribute or otherwise communicate any material which, in so doing, infringes copyright.

3.13 The use of language deemed aggressive, offensive or intimidating is not acceptable. You must not write anything on a website or send by email or other medium anything which could be reasonably be deemed offensive.

3.14 Use of a personal device to access any United Learning data is permitted, subject to the acceptance of the separate Bring Your Own Device policy.

3.15 Regard the use of Artificial Intelligence (AI) tools, including Generative AI, in the course of your work:

3.15.1 United Learning encourages the careful and considerate use of AI but advises using Generative AI tools cautiously.

3.15.2 AI presents significant opportunities but also carries inherent risks that necessitate awareness and mitigation.

3.15.3 School and trust safeguarding, data protection, cyber, internet use, and security policies are applicable to AI usage, including compliance with GDPR requirements. You must be familiar with and adhere to all related policies applicable to the use of AI.

3.15.4 Under no circumstances should any copyright protected, sensitive or Personal Identifiable Information (PII) be uploaded to paid-for or free-to-use generative AI models that are not Copilot. These operate in an unsecure, unprotected online environment without Enterprise Data Protection and any information provided may be used to train these generative AI models.

3.15.5 We encourage the use of Microsoft Copilot Chat (which has the same Enterprise Data Protection as all M365 products). For users who require more powerful AI tools, line managers can request the purchase of Microsoft 365 Copilot licences via the IT service. Please refer to our Policy on the Use of Microsoft 365 Copilot for more information.

3.15.6 You must not share Intellectual property (IP), such as United Learning curriculum resources with any premium paid-for or free-to-use Generative AI tool, for example asking it to generate a question set from a United Curriculum knowledge organiser, as the data that is uploaded may be used to train these generative AI models and it represents a breach of copyright.

3.15.7 Breach of this policy may result in disciplinary action.

3.16 Incident Reporting - Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the ICT Department in the first instance. If further action is required, this will be discussed with a member of the SMT.

3.17 Data Security - All staff are expected to secure devices with a password, this is mandatory for network user accounts and the locking of computers when leaving a desk is expected. Any phones, tablets or other devices that have access to school documents should be secured with a password or passcode and should never be left with an unauthorised person.

3.17.1 All staff are responsible for any activity on school systems carried out under access/account rights assigned to them, whether accessed via school ICT equipment or their own PC.

3.17.2 Screen displays should be kept out of direct view of any third parties when accessing personal, sensitive, confidential or classified information.

3.17.3 Staff should ensure they log off or lock their desktop before moving away from a computer during the normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorized access.

3.17.4 Staff must inform the Deputy Head/DSL or Network Manager if they receive an offensive e-mail.

3.18 The school allows pupils to use personal mobile devices occasionally on school trips.

Pupils agree to:

- Devices may be taken on away on school trips and long minibus trips (not matches)
- No photos are to be taken using a personal device, whilst in school. Photos may be taken on a trip if the staff member agrees and supervises. Photos may only be taken in appropriate areas. IE – not in rooms or bathrooms.
- Devices must have no phone capability; SIM cards must be removed.
- Any staff member allowing devices to be on their bus may check, with the owner present, that these rules are being observed.

The school is not responsible for the loss, damage or theft of any personal mobile device.

In KS1 pupils are taught Computer Science by the Network Manager, supported by the class TA. They are taught the following in an age-appropriate manner:

- How to use computer equipment correctly and safely.
- How to ask for help if they see or hear anything on the computer that upsets them or if they think something has gone wrong.
- They are taught explicitly about online bullying and inappropriate communications.
- To only use activities that the teacher has instructed them to.

*Staff must only use United Learning approved communication tools when discussing work or work related issues as the ICO (Information Commissioners Office) deem that private emails and messages when used for work purposes/communications are considered to be held by the organisation. Individuals would therefore be required to provide copies of these when United Learning responds to Subject Access Requests and Freedom of Information Act requests.