Lumen Learning Trust
Learning together for a brighter future

ICT User Agreement:
School Workforce
(includes Staff, Volunteers, Student placements, Directors, Governors & Contractors)

DATE APPROVED BY LUMEN LEARNING TRUST	14/07/2025		
REVIEW DATE [Biennial]	14/07/2027		
SIGNED DEPUTY EXECUTIVE PRINCIPAL	Sarah Kober 	**DATE**	14/07/2025
SIGNED CHAIR OF DIRECTORS	Jo Roberts 	**DATE**	14/07/2025

1. Aims & Background

This ICT user agreement covers the use of all digital technologies while *in school* including:

- Email
- Internet
- Intranet
- Network resources
- Learning platform
- Software
- Communication tools
- Social networking tools
- School website
- Apps
- Other relevant digital systems provided by the school or Local Authority
- Other information or systems processors
- Bring your own device (BYOD) hardware used to access any of the above

This ICT user agreement also covers school issued equipment (as logged on the asset register) when used *outside of school* including:

- Devices taken on school trips
- Online systems provided by the school such as VPN or webmail
- Other systems providers when accessed from outside school

This ICT user agreement also covers posts made on:

- Any non-school official social media platform or app, made from outside the school premises or school hours which reference the school or which might bring the professional status of a Lumen Learning Trust representative into disrepute.

The school regularly reviews and updates (with the assistance of the Data Protection Officer (DPO)) all user agreement documents to ensure that they are consistent with current school policies as listed at the end of the agreement.

2. Personal Responsibility

As a representative of the Trust you will accept personal responsibility for reporting misuse of ICT resources to a member of the applicable Senior Leadership Team. Misuse may come in many forms, but is commonly viewed as any information sent, received or viewed that indicates or suggests pornography, unethical or illegal activities, racism, sexism, inappropriate language or any use of which may be likely to cause offence.

3. Services

The Trust makes no guarantees of any kind, whether expressed or implied, for the ICT service that is provided. The Trust denies any responsibility for the validity or accuracy of any information obtained by its internet services. We do not recommend or endorse the storage of data outside of our network. If information is stored locally, for example on a laptop, the individual user is responsible for ensuring that their data is securely backed up.

4. Security

The security of our ICT services is very important. If you discover a security problem, please inform the Trust IT support provider as soon as possible.
Never try to replicate or demonstrate this problem to another user. All use of the ICT systems must be under your own username and password.
Anyone found to be sharing PC log in accounts and passwords may have their access blocked.
Any user identified as a security risk may have their access blocked and be subject to a disciplinary action.

5. Vandalism
Vandalism is defined as any malicious attempt to harm or destroy any equipment or data of another user or any other networks that are connected to the system. This includes but is not limited to, uploading and/or creation of computer viruses, the wilful damage of computer hardware and deletion of data.

6. Monitoring
All users email and system accounts have been provided to them by the Trust and should not be considered personal accounts. They are loaned to the individual for duration of the time employed by the Trust in order to undertake specific activities. The Trust reserves the right to monitor activity, using both automated systems (scanning for file types, file content) and manually. Where there is sufficient reason to do so appropriate individuals will be granted access to the accounts.

7. User Requirements

The school workforce using school systems must comply with the requirements below. Failure to do so could possibly mean disciplinary procedures being started.

Please note that school systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. Your behaviour online when in school and on all school devices whether in school or otherwise will be monitored by online safeguarding software.

a) I will only use the school's ICT resources and systems for professional purposes or for uses deemed 'reasonable' by the Headteacher and Executive Principal in the line of my employment.

b) I will set 'strong' passwords which is at least 8 characters and includes upper and lower case letters, numbers and symbols, following advice provided by the school or its ICT Support function. I will change it frequently. If I suspect it has been compromised I will change it immediately.

c) I will ensure that my computer is always in locked status when left unattended.

d) I will not reveal my password(s) to anyone. I will not disclose any passwords provided to me by the Trust or other related authorities.

e) I will not use anyone else's password if they reveal it to me and will advise them to change it.

f) I will not autosave my password or log in details for any Trust systems as this negates the effectiveness of the password.

g) I will not allow unauthorised individuals to access email / internet / intranet / network / social networks / mobile apps / or any other system I have access to via the school or other authority or processing system. I understand that anything undertaken while I am logged in, I will be held responsible for.

h) I will ensure all personal data is kept securely and is used appropriately whether in the workplace or working remotely. Documents, data, etc. will be printed, saved, accessed and deleted / shredded in accordance with the Trust and school's network and data security protocols, and retention policy.

i) I will not engage in any online activity that may compromise my professional responsibilities.

j) I will only use the schools approved email system(s) for any school business. I will always check if, and who, I should be cc'ing and bcc'ing and that the correct email address has been selected. Any attachments will be opened to check they are the correct file before sending.

k) I will not allow or apply any mail auto-forwarding tool to my Trust email address to allow onward transmission to an external, non-Trust email account.

l) *New for 2025* I understand that AI has many uses for teaching and learning as well as realising time efficiencies, but that it also poses risk to personal data. Therefore, I will:

- Familiarise myself with the LLT AI Acceptable Use Guidance for Staff.
- Never share or input any personal data to a free AI platform e.g. Chat GPT, DeepSeek, Google Gemini, Grammarly.

- Ensure before I use any AI tool it is reviewed and authorised by the Trust and only use it for the tasks which have been authorised.
- Understand that if I enter personal data into a free AI platform or into an AI Tool for a task which has not been authorised then it will either be considered a Data Breach or breach of this ICT User Agreement and could be subject to staff disciplinary proceedings.

m) I will only use the approved method/s of communicating with pupils or parents/carers and will only communicate with them in a professional manner and on appropriate school business.

n) I understand that WhatsApp is not an approved communication channel for the Trust. As it is not a Trust-controlled platform, the Trust is not able to monitor or easily access the information held. This can present issues if there were to be a Subject Access or Freedom of Information Request. Any existing WhatsApp group containing staff should not show any affiliation with the school via the name. The approved communication channels are school email system, parent mail and Google Chat. I will not use any form of social media as a communication tool in a professional capacity.

o) If I receive a suspicious email, I will report it to the Trust IT support provider before clicking on any links, downloading any attachments or entering my user details. When I report it, I will not forward the email but send a screen shot.

p) I will not support or promote extremist organisations, messages or individuals.

q) I will not give a voice or opportunity to extremist visitors with extremist views.

r) I will not browse, download or send material that could be considered offensive, illegal, discriminatory or of an extremist nature..

s) I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the Headteacher.

t) I will not download any hardware, software or resources from the internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed. I will seek advice from the Trust's IT support provider before making any download.

u) I will check copyright and intellectual property rights and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission. This includes the use of images taken from internet searches.

v) I will support the Trust's approach to online safety and not upload or add any images, video, audio or text linked to or associated with the Trust or its community onto my own social media platforms.

w) I will not transfer documents created and/or used within the Trust to, or allow use of these documents by, external organisations or persons without the express consent of the Executive Principal. This includes documents created by me or any other Lumen Learning Trust employee. Both as an existing Lumen staff member, or as an ex-employee, I am aware that I am prohibited from using the intellectual property of the Trust in any non-Trust endeavour.

x) I will not connect any device (including USB flash drive), to the network that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus and other malware systems.

y) I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home or on any personal devices.

z) I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the appropriate system or staff-only drive within school.

aa) I will only take or publish images of staff and students with their permission and in accordance with the school's policy on the use of digital / video images. Images published on the school website, online learning environment etc. will not identify students by name, or other personal information.

bb) I will use the school's Learning Platform or online cloud storage service in accordance with school protocols.

cc) I will ensure that any private social networking sites / blogs, etc. that I create or actively contribute to are not confused with my professional role, and will create a distinction between the two by ensuring there is no direct link with the Trust or school

dd) I will ensure, where used, I know how to use any official school or Trust social networking sites / tools securely e.g. Facebook, so as not to compromise my professional role.

ee) I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs. Under no circumstances should the operating system or installed applications on any school provided devices be modified by the user in any way.

ff) I will only access school resources remotely (such as from home) using the school approved RDS system and follow e-security protocols to interact with them.

gg) I will transfer any sensitive or special category data, which might include SEND, EHCP, medical or health information, criminal record data or financial information, to non-Lumen Learning Trust email accounts using appropriate protection and/or encryption. This includes referring to individuals by their initials only within emails in every instance and/or using Egress.

hh) I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.

ii) I understand that the Lumen data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

jj) I am aware that under the provisions of the Data Protection Act 2018 and UK General Data Protection Regulations, my school and I have extended responsibilities regarding the creation, use, storage and deletion of data, and I will not store any pupil data that is not in line with the school's data retention policy and adequately protected. The school's DPO must be aware of all data storage.

kk) I understand that anything I write in an email or document about an identifiable person can be requested via a Subject Access Request and read by that individual. Therefore, I will not write anything that I would not want that person to read, could bring the organisation into disrepute or runs counter to the Lumen Learning Trust Staff Code of Conduct.

ll) I will consider if the communication I send breaches confidentiality or the Data Protection Act by asking myself "should the recipient view this information".

mm) I understand that I can cause a Data Protection breach by destroying or corrupting data and all data should be held in line with the Trust's data retention schedule.

nn) I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to a member of SLT or a Designated Safeguarding Lead.

oo) I understand that all internet and network traffic / usage can be logged and this information can be made available to the Headteacher on their request.

pp) I will not use the Trust's ICT systems for any commercial activities, such as work for a for-profit organisation.

qq) When using personal devices I will ensure that anti-virus protection is in place that has been updated to limit potential vulnerabilities.

rr) I understand that all inbound and outbound calls are recorded for training and monitoring purposes. Appropriately authorised individuals may review calls where deemed appropriate. Therefore, personal calls made on school devices could be listened to. When it becomes apparent that it is a personal call the reviewer will immediately cease listening to the recording, unless it is directly related to the reasons for the review.

ss) I understand that internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.

tt) I understand that I have a responsibility to uphold the standing of the teaching profession and of the school, and that my digital behaviour can influence this.

uu) *Workforce staff with a teaching role only:* I will embed the school's online safety / digital literacy / counter extremism curriculum into my teaching.

vv) *Workforce staff with a governance role only*:

- Governance documentation will be stored electronically on the governance shared drives, online document portal GovernorHub or securely in hard copy in line with the Trust's Data Retention policy.
- Any information downloaded from shared drives onto a personal device should be deleted upon the completion of the task, including from temporary internet files and Download folders.
- Only Trust provided email accounts should be used for Trust business. This prevents subject access requests to personal email accounts and facilitates compliance with any email retention period.
- I note that any email account can be monitored by appropriate individuals if there is due cause.

8. Links with Other Policies

I understand that this user agreement is linked to the schools:

- Freedom of information publication scheme
- Email Security and Etiquette Guidance
- Social Media for School Staff Policy
- Social Media for Schools Policy
- Data Protection Policy
- Loan of ICT Equipment to Staff agreement
- Staff Code of Conduct
- Staff Handbook
- Data Retention Policy
- Breach Management Policy
- Asset Management Recording Policy
- Disaster Recovery/Business Continuity Planning and Risk Register
- Safeguarding and Child Protection Policy
- Low Levels Concerns Policy
- Capturing and Storing Images Policy

9. Agreement Form

User Signature

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others' e-safeguarding and I undertake to be a 'safe and responsible ICT user'.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent online safety / safeguarding policies.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature: _____

Full Name (printed): _____

Job title/role: _____

Date: _____

Authorised Signature (Headteacher / Deputy)

I approve this user to be set-up on the school systems relevant to their role:

Signature: _____

Full Name (printed): _____

Date: _____