CAMBRIAN

Nurturing Growth - Inspiring Minds

IT Acceptable Use Policy for Staff

V1.9

This document applies to all academies and operations of Cambrian Learning Trust.

www.cambrianlearningtrust.org

Document Control			
Author	COO	**Approved By**	COO
Last Reviewed	18/07/2022	**Next Review**	18/07/2025
Review Cycle	3 years	**Version**	1.9

Contents

Guidelines for Staff

Cambrian Learning Trust has provided computers and devices for use by staff as an important tool for teaching, learning, and administration of the school. Use of CLT computers and devices by members of staff is governed at all times by the following policy.

Pupils sign a pupil ICT Code of Conduct.

Please ensure you understand your responsibilities under this policy and direct any questions or concerns to the ICT Services Team in the first instance.

All members of staff have a responsibility to use the school's ICT system in a professional, lawful, and ethical manner.

Any deliberate disregard OR breach of this policy may result in disciplinary action (including possible termination), and civil and/or criminal liability.

Please note that use of the school network is intended to be as permissive and flexible as possible under current UK legislation and DfE guidelines. This policy is not intended to arbitrarily limit the ways in which you can use the system, but to ensure compliance with the legal responsibilities of the school and staff, to safeguard the reputation of the school, and to ensure the safety of all users. Please respect these guidelines, many of which are in place for your protection.

The school recognises that the distinction between computer use at work and at home is increasingly blurred, with many of us now using our own computers or mobile devices for work. While CLT neither wishes nor intends to dictate how you use your own devices, staff should consider that the spirit of this policy applies whenever you are undertaking an activity that stems from your employment within the Trust/ school.

Please note: When logging onto Cambrian Learning Trust ICT System you are agreeing to this Acceptable Use Policy.

Computer Security and Data Protection

- All activity **must** be carried out with a clear understanding of GDPR.

  You will be provided with a personal account for accessing the computer system, with your own username and password. This account will be tailored to the level of access you require and is for your use only. As such, **you must not disclose any workplace password to anyone, including to ICT services.**

- You **must not allow a pupil to have individual use of a staff account** under any circumstances, for any length of time, even if supervised.
- When leaving a device unattended, you **must** ensure you have either logged off your account or locked the device to prevent anyone using your account in your absence.
- You **must not** store any sensitive or personal information about staff or students on any portable storage system (such as a USB memory stick, portable hard disk, or personal computer or device) unless that storage system is encrypted and approved for such use by the Trust.
- You **must not** transmit any sensitive or personal information about staff or students via email. Please note SIMS, or equivalent, can be used to store and share information. **Please note:** during the transition period to SharePoint, whilst file structures are being determined, sharing and copying links may be restricted. **If** this is the case, files may be downloaded and shared via email **where necessary.**
- When publishing or transmitting non-sensitive material outside of the Trust, you **must** take steps to protect the identity of any pupil whose parents have requested this.
- If you use a personal computer or device at home for work purposes, you **must** ensure that any school-related sensitive or personal information is secured to prohibit access by any non-member of staff.
- You **must** ensure that items of portable computer equipment (such as laptops, digital cameras, or portable projectors) are securely stored in a locked room or cupboard when left unattended.
- Equipment taken offsite is not routinely insured by the Trust or the school. If you take any Trust computer equipment offsite, you should ensure that adequate insurance cover has been arranged to cover against loss, damage, or theft.

Office 365

- As a Trust, all Staff and Students have access to Office 365. This is web based and can be accessed via the internet.
- ICT Services can view and manage usage where necessary.
- ICT Services can run reports on individual users if required. These reports can be individually customised but can only be created on authority from the Trust SLT.

- When using SharePoint, you **must** ensure caution is used on sharing files or folders, or copying links, whether internally or externally. Staff **must** ensure they use correct contacts and permissions. Prior to sharing files or folders or sending a link to a file or folder, consideration **must** be given as to the reason for sharing. If using this method, the share folder/ file is permanent unless the sharer amends the permissions. **Please note:** during the transition period to SharePoint, whilst file structures are being determined, sharing and copying links may be restricted. **If** this is the case, files may be downloaded and shared via email **where necessary.**
- It may be more appropriate to provide the recipients with permission to access to that specific file or folder on a permanent basis, if they do not already have access to that area. If using this method, the share folder/ file is permanent unless the sharer amends the permissions. Permission to access an area can be requested via ICT Services and should be agreed with the line manager.
- It is recommended that One Drive should only be used for **personal** files such as appraisals, training records and other files which relate to you personally.
- No files which contain student data can be saved in One Drive.
- SharePoint should be used for all Teacher Documents and Resources in the relevant area.
- Any change of access to E-Mails and/or SharePoint sites, a Change Request needs to be completed prior to ICT Services actioning.
- Users who use Office 365 are also liable to Microsoft's Terms and Conditions https://www.microsoft.com/en-gb/servicesagreement/default.aspx

Use of Email

All members of staff with a computer account are provided with an email address for communication both internally and with other email users outside the Trust. The following considerations must be made when communicating by email:

- E-mail has the same permanence and legal status as written hardcopy (paper) documents and may be subject to disclosure obligations in exactly the same way. Copies of e-mails may therefore have to be made available to third parties. You **must** be cautious when sending both internal and external mails. The professional standards that apply to internal memos and external letters must be observed for e-mail.

- E-mail to outside organisations has the same power to create a binding contract as hardcopy documents. Check e-mail as carefully as written contracts, always use a spell checker and, where appropriate, obtain legal

advice before sending. You **must not** purchase goods or services on behalf of the Trust via e-mail without proper authorisation.

- All group E-mails, where the recipients are based at different locations / sites, and especially when the group includes external email addresses from outside of the trust. **Should be sent as bcc**. This includes Outlook Calendar invitations. Full details on how to do this can be found in **Appendix I** - *GDPR and BCC in Outlook and M365 guide.*

- E-mail is not a secure method of communication, and can be easily copied, forwarded and archived. Unless explicitly authorised to do so, you **must not** send, transmit, or otherwise distribute proprietary information, copyrighted material, trade secrets, or other confidential (i.e. data) information belonging to Cambrian Learning Trust. **Please note:** during the transition period to SharePoint, whilst file structures are being determined, sharing and copying links may be restricted. **If** this is the case, files may be downloaded and shared via email **where necessary.**

- Having an external e-mail address may lead to receipt of unsolicited e-mail containing offensive and/or sexually explicit content. IT Services will take measures to minimise the receipt and impact of such content, but cannot be held responsible for material viewed or received by users from the Internet.

- You must not send chain letters or unsolicited commercial e-mail (also known as SPAM).

- Staff **must** be cautious when opening an email from an external source. If there is a doubt that the email is suspicious it should **not** be forwarded. Any questions, on the reliability of the email should be directed to the IT Services Team.

Leavers

When a member of staff resigns from their employment with the Trust, it is the employee's responsibility, in liaison with their line manager, to adapt their email signature such that it contains appropriate wording to inform respondents that they are leaving their position. Advice should be sought from HR if there is any uncertainty over the leaving date. The amendment to the email signature should state that the mailbox will no longer be accessed after the leaving date and an alternative email address provided for the sender to forward any emails to. This will be as directed by their line manager. It is the employee's responsibility, in discussion with their line manager to save or forward any emails from their mailbox, as appropriate and in line with GDPR guidelines, that may need to be referenced again.

On the leaving date, it is the employee's responsibility, in liaison with their line manager, to create an automated reply / out of office message to both internal and external recipients stating that the mailbox is no longer accessed and that with immediate effect the sender should re-send any emails to an alternative mailbox e.g. named manager or colleague, as determined by their line manager.

Employee email accounts will remain open for one calendar month, after the termination of employment date to facilitate the delivery of the automated reply message. After one calendar month, the email account will be deleted. Upon deletion of the email account, an automated "bounce back" message will be sent from Microsoft with an undeliverable status.

In exceptional circumstances, if access to an individual's mailbox is needed for specific, time limited, business reasons after the termination of employment then IT services will seek agreement from the relevant Head Teacher or Chief Operating Officer before granting access.

Password Policy

The password policy is:

- Passwords must be at least 10 characters long and use three of the following four categories:
    - Uppercase letter
    - Lowercase letter
    - Number
    - Symbol

- Your password cannot contain your name
- The new password cannot be one of your previous 5 passwords
- Passwords will prompt you to change every 101 days

For those managing access for supply staff, visitors and contractors that require temporary access to school systems you **must** ensure their password is changed on a daily basis. This is for security reasons to prevent unauthorised access to data whilst off site outside of school hours.

Internet Usage

Whilst Users are using the Trust internet, on any device, websites are monitored.

Certain sites, eg social media sites, are blocked in line with Trust policy.

Personal Use

Cambrian Learning Trust recognises that occasional personal use of the Trust's devices is beneficial both to the development of ICT skills and for maintaining a positive work-life balance. Such use is permitted, with the conditions that such use:

- **must** comply with all other conditions of this AUP as they apply to non-personal use, and all other Trust policies regarding staff conduct;
- **must not** interfere in any way with your other duties or those of any other member of staff;
- **must not** have any undue effect on the performance of the computer system; and
- **must not** be for any commercial purpose or gain unless explicitly authorised by Cambrian Learning Trust.

Personal use is permitted at the discretion of the Trust and can be limited or revoked at any time.

Use of your own Equipment

- Any mains-operated personal computer or electrical equipment brought on site, for any use, is subject to a Portable Appliance Test (PAT) by site maintenance staff, and **must not** be used until approved. This test must be performed at regular intervals as required by the Trust's normal rules on electrical safety testing.
- You **must not** connect personal computer equipment to Trust computer equipment without prior approval from the IT Services Team, with the exception of storage devices such as USB memory sticks.
- If you keep files on a personal storage device (such as a USB memory stick), you **must** ensure that other computers you connect this storage device to

(such as your own computers at home) have an up-to-date anti-virus system running to protect against the proliferation of harmful software onto the Trust computer system.

- If using own equipment for work whilst at home, staff members **must** take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:
    - Keeping the device password-protected
    - Accessing and saving any work via Office 365 rather than on the device
    - Making sure the device locks if left inactive for a period of time
    - Installing antivirus and anti-spyware software
    - Keeping operating systems up to date

Conduct

1. You **must** at all times conduct your computer usage professionally, which includes being polite and using the system in a safe, legal and business appropriate manner. Among uses that are considered unacceptable are the following:
    a. Using, transmitting, or seeking inappropriate, offensive, pornographic, vulgar, suggestive, obscene, abusive, harassing, threatening, racist, sexist, or defamatory language or materials;
    b. Making ethnic, sexual-preference, or gender-related slurs or jokes
2. You **must** respect, and not attempt to bypass, security or access restrictions in place on the computer system.
3. You **must not** intentionally damage, disable, or otherwise harm the operation of equipment.
4. You **must** make efforts not to intentionally waste resources. Examples of resource wastage include:
    a. Excessive downloading of material from the Internet;
    b. Excessive storage of unnecessary files on the network storage areas;
    c. Use of computer printers to produce class sets of materials, instead of using photocopiers.
5. You should avoid eating or drinking around computer equipment.

6. When live / remote teaching from home, staff **must** ensure they are conducting online lessons in a suitable environment for learning.

Use of Social Networking forums for work related activity

Increasingly workplaces/ work groups are using social media and messaging platforms for communication. This includes, but it not exclusive to, WhatsApp. However, increasingly there are workplace issues arising from the use of these tools.

This is in 2 specific areas:

1. Managing grievances and claims for bullying and harassment

   These claims commonly arise from

   - Being excluded from groups and plans
   - Gossip or banter and inappropriate language in messages
   - Inappropriate pictures or videos being shared

   This could lead to successful claims of unlawful discrimination under the Equality Act 2010. Staff need also be aware that they personally could be liable for bullying and harassment claims and could be exposed to civil or criminal complaints under the Protection from Harassment Act 1997.

2. Confidentiality and Data breaches

   Where communications slip into work related messages, these could be disclosed in the context of any subsequent regulatory enquiry or litigation.

   It should also be noted that WhatsApp messages may need to be disclosed in a Subject Access Request.

   WhatsApp must not be used to share any information that is defined as employee or pupil data.

   Whilst the Trust recognises that it cannot ban the use of WhatsApp work groups it strongly advises that is follows the same guidelines as laid down in this policy

Use of Social Networking websites and online forums

Staff must take care when using social networking websites such as Facebook, Instagram or Twitter, even when such use occurs in their own time using their own computer. Social Networking sites invite users to participate in informal ways that can leave you open to abuse, and often make little or no distinction between adult users and children.

You **must not** allow any pupil to access personal information you post on a social networking site. In particular:

- You **must not** add a pupil to your 'friends list'.
- You **must** not accept or initiate a friendship request on social media from a parent unless there is a personal relationship.
- You **must** ensure that personal information is not accessible via a 'Public' setting, but ensure it is set to a 'Friends only' level of visibility.
- You **must** avoid contacting any pupil privately via a social networking website, even for School-related purposes.
- You **must** take steps to ensure that any person contacting you via a social networking website is who they claim to be, and not an imposter, before allowing them access to your personal information.

Staff **must** also take care when posting to any public website (including online discussion forums or blogs) that their comments do not harm their professional standing or the reputation of Cambrian Learning Trust – even if their online activities are entirely unrelated to the trust.

- Unless authorised to do so, you **must not** post content on websites that may appear as if you are speaking for the Trust.
- You should not post any material online that can be clearly linked to Cambrian Learning Trust that may damage the Trust's reputation.
- You **must** avoid posting any material clearly identifying yourself, another member of staff, or a pupil, that could potentially be used to embarrass, harass, or defame the subject.

Supervision of Pupil Use

- Pupils **must** be supervised at **all** times when using Trust devices. When arranging use of computer facilities for pupils, you must ensure supervision is available
- Supervising staff are responsible for ensuring that the IT Code of Conduct for

pupils is enforced.

- Supervising staff **must** ensure they have read and understand the separate guidelines on e-safety, which pertains to the child protection issues of computer use by pupils.

Privacy

- Use of the Trust Computer System, including your email account and storage areas provided for your use, may be subject to monitoring by the ICT Services Team or Senior Leadership Team, to ensure compliance with this Acceptable Use Policy and applicable laws. This may include remote monitoring of an interactive logon session.
- You should avoid storing sensitive personal information on the Trust computer system that is unrelated to Trust activities (such as personal passwords, photographs, or financial information).
- The ICT Services Team and/or SLT may also use measures to audit use of computer systems for performance and diagnostic purposes.
- Use of the Trust computer system indicates your consent to the above described monitoring taking place.

Confidentiality and Copyright

- Respect the work and ownership rights of people outside the Trust, as well as other staff or pupils.
- You are responsible for complying with copyright law and licenses that may apply to software, files, graphics, documents, messages, and other material you wish to use, download or copy. Even if materials on the Trust computer system or the Internet are not marked with the copyright symbol (©), you should assume that they are protected under copyright laws unless there is an explicit permission on the materials to use them.
- You **must** consult a member of ICT Services Team before placing any order of computer hardware or software, or obtaining and using any software you believe to be free. This is to check that the intended use by the Trust is permitted under copyright law (as well as to check compatibility and discuss any other implications that the purchase may have). Do not rely on the claims of suppliers, who do not have specific knowledge of the Trusts' systems.
- As per the standard staff contract, any invention, improvement, design, process, information, copyright work, trade mark or trade name made, created

or discovered by you during the course of your employment in any way affecting or relating to the business of the Trust or capable of being used or adapted for use within the Trust. This shall be immediately disclosed to the Trust and shall to the extent permitted by law belong to and be the absolute property of the Trust.

- By storing or creating any personal documents or files on the Trust computer system, you grant Cambrian Learning Trust a non-exclusive, universal, perpetual, irrevocable, and royalty-free license to use, copy, and distribute those documents or files in any way the school sees fit.

Reporting Problems with the Computer System

It is the job of the ICT Services Team to ensure that the Trust computer system is working optimally at all times and that any faults are rectified as soon as possible. To this end:

- You should report any problems that need attention to a member of IT Services Team as soon as is feasible. Issues should be reported via the helpdesk system where possible.
- If you suspect your computer has been affected by a virus or other malware, you **must** report this to a member of the ICT Services Team **immediately**. The Computer needs to be shutdown to prevent the spread of any potential attacks.
- If you have lost documents or files, you should report this as soon as possible. The longer a data loss problem goes unreported, the lesser the chances of your data being recoverable.

Reporting Breaches of this Policy

All members of staff have a duty to ensure this Acceptable Use Policy is followed. You **must** immediately inform a member of the ICT Services Team, or the Headteacher, of abuse of any part of the computer system. In particular, you should report:

- Any websites accessible from within the Trust that you feel are unsuitable for staff or student consumption;
- Any inappropriate content suspected to be stored on the computer system. This may be contained in email, documents, pictures, etc
- Any breaches, or attempted breaches, of computer security; or

- Any instance of bullying or harassment suffered by you, another member of staff, or a pupil via the Trust computer system

Reports should be made The Support Helpdesk System. All reports will be treated confidentially.

Review and Evaluation

This policy will be reviewed every two years by the Trust ICT Manager and in response to any changes affecting the basis of the original risk assessment, for example: significant security incidents, new vulnerabilities and significant changes to the organisation or technical infrastructure. Changes to this policy will be communicated to all staff.

Notes

"Sensitive personal information" is defined as information about an individual that is protected by law under the Data Protection Act 2018. Examples of such data include addresses and contact details of individuals, dates of birth, and pupil SEN data.

This list is not exhaustive. Further information can be found in the school's Data Protection Policy.

Acceptance of this policy

This policy is stored within the Edupay document folder and it is mandated that it is read. You may be requested, on an annual basis, to confirm your understanding.