CAMBRIAN

Nurturing Growth - Inspiring Minds

IT Acceptable Use Policy for Staff

Last reviewed: September 2021

This document applies to the following schools:

Charlton Primary School
King Alfred's Academy
Larkmead School
Millbrook Primary School
St James CE Primary School
St John's CE Academy
St Nicholas CE Primary School
Thameside Primary School
Wantage CE Primary School

www.cambrianlearningtrust.org

Document Control			
Author	Head of Governance	**Approved By**	Trust Board
Last Reviewed	September 2021	**Next Review**	September 2023
Review Cycle	2 years	**Version**	2021

Contents

1. Terminology used in this policy

- "**Trust**", "**we**" and "**our**" means the Cambrian Learning Trust, inclusive of its schools and operations.
- "**parent**" means parent, carer or other adult with parental responsibility
- "**user**" and "**user community**" means pupils, parents, staff, governors, trustees, members, volunteers, contractors, visitors and others authorised to use our ICT resources
- "**ICT resources**" means all of our Information and Communications (ICT) devices, systems and services including but not limited to network infrastructure, Internet access, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device, system or service which may become available in the future which is provided as part of or through our ICT resources.
- "**materials**" means files and data created, used or transmitted using the ICT resources including but not limited to messages, emails, documents, photos, audio, video, printed output, web pages, social networking, vlogs and blogs.
- "**personal use**" means use or activity not directly related to a user's employment, study or other bona-fide Trust or school related purpose.
- "**authorised personnel**" means employees authorised by the Trust to perform administration and/or monitoring of the ICT resources.
- "**social media**" means all websites and applications that enable users to create and share content or to participate in social networking or messaging. For avoidance of doubt, this includes Facebook, YouTube, WhatsApp, Facebook Messenger, Instagram, Twitter, Telegram, Slack, MS Teams, Snapchat, Reddit, Pinterest, TikTok, SMS, Zoom and all similar platforms and any that may become available in the future.

2. Related policies and procedures

This policy should be read alongside our policies and procedures on.

- Safeguarding and child protection
- Behaviour management
- Anti-bullying
- Online safety

- Data protection
- Social media
- Staff discipline
- Staff code of conduct

3. Purpose of this policy

The purpose of the policy is to:

- Set guidelines and rules for the user community on the use of our ICT resources.
- Establish clear expectations for the way users engage with one another online.
- Support our policies and procedures on safeguarding, online safety, behaviour, conduct and data protection**.**
- Prevent disruption to our operations through the misuse, or attempted misuse, of our ICT resources.

4. Unacceptable use

The following is considered unacceptable use of our ICT resources by any user:

- Breaching any of our policies or procedures.
- Bullying or harassing or promoting unlawful discrimination.
- Using inappropriate or offensive language.
- Any illegal conduct, or statements which are deemed to be advocating illegal activity**.**
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate.
- Activity which defames or disparages the school, or the Trust, or individuals, or risks bringing the school, or the Trust, or individuals into disrepute.
- Unauthorised sharing of confidential data about the Trust or the school.
- Causing a data breach by accessing, modifying, or sharing personal data without authorisation.
- Breaching intellectual property rights or copyright.
- Connecting any device to our ICT network without approval from authorised personnel.

- Using websites or mechanisms to bypass our filtering and firewall mechanisms.
- Setting up or using any software, applications or web services on our network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the operation of the ICT resources, accounts or data.
- Gaining or attempting to gain access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel.
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to our ICT resources.
- Causing intentional damage to our ICT resources.
- Removing, deleting or disposing of ICT resources or materials without permission from authorised personnel.
- Promoting a private business, unless that business is directly related to the Trust, or a Trust school, and permission has been given in advance by a senior Trust executive or the appropriate headteacher.

This is not an exhaustive list and we reserve the right to amend it at any time, without notice. We will use our professional judgement to determine whether any act or behaviour not on the list above is considered an unacceptable use of our ICT resources.

Any member of the user community who engages in any unacceptable activity may be sanctioned in line with our policies on behaviour, discipline, or an appropriate code of conduct, or an appropriate contract.

5. Staff

*Including employees, governors, trustees, members, volunteers and contractors

5.1. Access to ICT resources and materials

Authorised personnel manage access to our ICT resources and materials for staff. This includes, but is not limited to:

- Provision of computers, tablets and other devices
- Access permissions for certain systems, programmes or files

Staff will be provided with unique log-in/account information and passwords that they must keep safe and use when accessing our ICT resources.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should notify authorised personnel or their line manager.

Email

Every member of staff is issued with an email address which should be used for work purposes only.

Staff must not send any work-related materials using their personal email accounts, nor share their personal email addresses with parents and pupils.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages may be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 and the UK GDPR in the same way as paper documents. Deletion from a user's inbox does not mean that an email message cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error which contains the personal information of another person, they must inform their line manager immediately and follow our data breach procedure.

Phones

Staff must not give their personal phone numbers to parents or pupils.

Staff who are provided with work mobile phones must abide by the same rules for acceptable use as set out in this policy when using these phones.

Work mobile phones must not be used for personal matters, except on a very occasional or emergency basis.

5.2. Personal use

Staff are permitted to occasionally use our ICT resources for personal use subject to certain conditions set out below. Personal use of ICT resources must not be overused or abused. We may withdraw permission for it at any time or restrict access at our discretion.

Personal use is permitted provided that such use:

- Does not take place during work hours or when on duty or during non-break time
- Does not constitute 'unacceptable use', as defined in this policy
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the resources for work or educational purposes

Staff may not use our ICT resources to store personal non-work-related information or materials (such as music, videos, or photos).

Staff should be aware that use of our ICT resources for personal use may put personal communications within the scope of our ICT monitoring activities.

Staff use of personal devices (such as mobile phones or tablets) in work time and/or on work premises must be in accordance with their local workplace policy concerning these matters.

Staff should be aware that personal use of ICT (even when not using our ICT resources) can impact on their employment by, for instance putting personal details in the public domain, where pupils and parents could see them.

Staff should follow the guidance in this and related policies concerning the use of social media and email, and take care to protect themselves online to avoid compromising their professional integrity.

Personal social media accounts

Members of staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times and in accordance with the Trust's Social Media Policy.

5.3. Remote access

Staff accessing our ICT resources and materials remotely must abide by the same rules as those accessing the resources and materials on-site. Staff must abide by

the guidance and protocols provided by the Trust/School covering remote learning. Staff must be particularly vigilant if they use our ICT resources outside Trust/school premises and take such precautions as we may advise from time to time against importing viruses or compromising system security.

Our ICT resources and materials contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy, a copy of which can be found on Trust and school websites.

5.4. School and Trust official social media accounts

Staff members who have not been authorised to manage, or post to, official school or Trust social media accounts must not access, or attempt to access these accounts.

Activity on official social media accounts must be in compliance with the Trust's Social Media Policy.

5.5. Monitoring of network and use of ICT resources

We reserve the right to monitor the use of its ICT resources and network. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

We may monitor ICT use in order to:

- Obtain information related to our business
- Investigate compliance with policies, procedures and standards
- Ensure effective ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime

- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

6. Pupils

6.1. Access to ICT resources and materials

Each school in the Trust has its own local procedures concerning pupil access to ICT resources. These may include, for example:

- Computers and equipment either provided in the classroom or the school's ICT suite, available to pupils only under the supervision of staff
- Specialist ICT equipment, such as that used for music or design and technology, which must only be used under the supervision of staff
- Pupil accounts linked to the school's virtual learning environment

6.2. Search and deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, we have the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under legislation or our rules.

We can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break our rules.

6.3. Unacceptable use of ICT and the internet outside of school

We will sanction pupils, in line with our behaviour policy and procedures, if a pupil engages in any of the following at any time (even if they are not on school premises):

- Using ICT or the Internet to breach intellectual property rights or copyright
- Using ICT or the Internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching our policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate

- Activity which defames or disparages the school or Trust, or risks bringing the school or Trust into disrepute
- Sharing confidential information about the school or Trust, other pupils, or other members of the user community
- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to our ICT resources or materials
- Causing intentional damage to our ICT resources or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

7. Data security

We take steps to protect the security of our ICT resources and materials, however we cannot guarantee security, therefore it is essential that everyone in the user community uses safe computing practices at all times.

7.1. Passwords

All users should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action.

Parents or volunteers who disclose account or password information may have their access rights revoked.

7.2. Software updates, firewalls, and anti-virus software

All of our ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we put in place to protect personal data and our ICT resources.

7.3. Data protection

All personal data must be processed and stored in line with data protection regulations and our data protection policy and related procedures, which can be found on Trust and school websites and intranets.

7.4. Access to resources and materials

All users of our ICT resources will have clearly defined access rights to certain systems, files and devices. These access rights are managed by authorised personnel.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should immediately alert their teacher or line manager, as appropriate, who in turn should escalate the matter to authorised personnel.

Devices and systems should always be logged out of and closed down completely at the end of each session, and devices should be locked away to help avoid loss or unauthorised access.