Launceston College

A Multi Academy Trust

Staff acceptable use policy

Adopted on	**8 February 2021**
Ratified by	**Finance & Assets Committee**
Status	**Ratified**
Review period	**Every 2 Years**
Review date	**February 2023**

Contents

1. Introduction and aims 1
2. Relevant legislation and guidance 1
3. Definitions.. 1
4. Unacceptable use 2
5. Staff (including governors, volunteers, and contractors) 3
6. Pupils...Error! Bookmark not defined.
7. Parents ....Error! Bookmark not defined.
8. Data security 4
9. Internet access.. 5
Appendix 1: Facebook cheat sheet for staff 6

1. 1. Introduction and aims

ICT is an integral part of the way our school and trust works, and is a critical resource for pupils, staff, governors, trustees, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions.

However, the ICT resources and facilities we use also poses risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of ICT resources for staff, pupils, parents and governors
- Establish clear expectations for the way all members of the trust engage with each other online
- Support the trust's policy on data protection, online safety and safeguarding
- Prevent disruption to the school/trust through the misuse, or attempted misuse, of ICT systems
- Support the school and trust in teaching pupils safe and effective internet and ICT use

This policy covers all users of our ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our disciplinary policy.

2. 2. Relevant legislation and guidance

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

- Data Protection Act 2018
- The General Data Protection Regulation
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2018
- Searching, screening and confiscation: advice for schools

3. 3. Definitions

- **"ICT facilities":** includes all facilities, systems and services including but not limited to network infrastructure, 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 the ICT service from the school or trust

- **“Users”:** anyone authorised by the trust/school to use the ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors
- **“Personal use”:** any use or activity not directly related to the users’ employment, study or purpose
- **“Authorised personnel”:** employees authorised by the school/trust to perform systems administration and/or monitoring of the ICT facilities
- **“Materials”:** files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs

4. 4. Unacceptable use

The following is considered unacceptable use of the ICT facilities by any member of the school/trust community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the school/trust’s ICT facilities includes:

- Using ICT facilities to breach intellectual property rights or copyright
- Using ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school/trust’s 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/trust, or risks bringing either into disrepute
- Sharing confidential information about the school/trust, its pupils, or other members of the community
- Connecting any device to the ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the ICT network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, 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 the ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- 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
- Promoting a private business
- Using websites or mechanisms to bypass the Internet filtering mechanisms

This is not an exhaustive list. The school/trust reserves the right to amend this list at any time. The principal or trust ICT Manager will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of ICT facilities.

4.1 Exceptions from unacceptable use

Where the use of ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the trust ICT manager’s discretion.

If in doubt, please raise a ticket through your IT support helpdesk.

4.2 Sanctions

Staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies.

5. 5. Staff (including governors, volunteers, and contractors)

5.1 Access to school ICT facilities and materials

The school's IT site supervisor and the trust ICT IT manager manage access to ICT facilities and materials for staff. That includes, but is not limited to:

- Computers, tablets and other devices
- Access permissions for certain programs or files

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

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should raise a ticket with their IT helpdesk.

5.1.1 Use of phones and email

The school/trust provides each member of staff with an email address which should be used for work purposes only.

All work-related business should be conducted using the email address the school/trust has provided.

Staff must not share their personal email addresses with parents or students and must not send any work-related materials to or from their personal email account.

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 are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email 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 email or attachments containing personally identifiable information about other staff or students that is sent outside the trust 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 the ICT site supervisor immediately and follow the data breach procedure.

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

Work phones must not be used for personal matters.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

In-coming and out-going phone conversations may be recorded for training and monitoring purposes.

5.2 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.

The school/trust has guidelines for staff on appropriate security settings for Facebook accounts (see appendix 1).

5.3 Remote access

Staff accessing ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use ICT facilities outside the school/trust and take such precautions against importing viruses, compromising system security and GDPR/data security.

Our ICT facilities 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.

5.4 School social media accounts

Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

The school/trust has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

5.5 Monitoring of school network and use of ICT facilities

The school/trust reserves the right to monitor the use of its ICT facilities 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.

The school/trust monitors ICT use in order to:

- Obtain information related to school/trust business
- Investigate compliance with policies, procedures and standards
- Ensure effective school/trust and 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. Data security

The school takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Staff, pupils, parents and others who use ICT facilities should use safe computing practices at all times.

6.1 Passwords

All users of the ICT facilities 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.

6.2 Software updates, firewalls, and anti-virus software

All of the 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 implement and maintain to protect personal data and ICT facilities.

Any personal devices using the school’s network must all be configured in this way.

6.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the school’s data protection policy.

6.4 Access to facilities and materials

All users of the ICT facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed by the ICT site supervisor.

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 alert their ICT site supervisor immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

6.5 Encryption

The school ensures that its devices and systems have an appropriate level of encryption.

Staff may not store school data on personal devices (eg computers and USB drives).

7. Internet access

The school/trust wireless internet connection is secured and is setup to provide different levels of filtering depending on the role of the user, however filters aren’t fool-proof so users should take appropriate care.

1.1.1 Appendix 1: Facebook cheat sheet for staff

Don’t accept friend requests from pupils on social media

10 tips school staff on Facebook

1. Consider changing your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don’t share anything publicly that you wouldn’t be just as happy showing your pupils
6. Don’t use social media sites during school hours
7. Don’t make comments about your job, your colleagues, our school or your pupils online – once it’s out there, it’s out there
8. Don’t associate yourself with the school on your profile (e.g. by setting it as your workplace, or by ‘checking in’ at a school event)
9. Don’t link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises wifi connections and makes friend suggestions based on who else uses the same wifi connection (eg pupils)

Check your privacy settings

- Change the visibility of your posts and photos to **‘Friends only’**, rather than ‘Friends of friends’. Otherwise, pupils and their families may still be able to read your posts, see things you’ve shared and look at your pictures if they’re friends with anybody on your contacts list
- Don’t forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you’ve **‘liked’**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can’t **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What do to if…

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you’re not allowed to accept friend requests from pupils and that if they persist, you’ll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages and speak to your line manager and DSL.

A parent adds you on social media

- Decline the offer or ignore the message. Contact with parents should be via professional channels, eg work email.

You’re being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police