Carlton Academy Trust

Staff Code of Conduct, Social Media and ICT Acceptable Use Policy

Ratified Date:	Sept 2020
Signed on behalf of the Trustees:	G Logan
Signed on behalf of the CEO:	A Kneeshaw
Review Date:	Sept 2023

Scope and Policy Aims

This policy applies to all staff, trustees/governors, volunteers, contractors and visitors, and aims to encourage and guide the highest standards of professionalism and conduct so that the trust can set and maintain a positive example to students, school and wider community.

Dignity at Work

CAT is committed to eliminating harassment and bullying to create a productive working environment where everyone is treated with respect. All harassment and bullying are unacceptable, and all employees have a duty to behave in a professional and appropriate manner to ensure this.

Dress Code

Staff act as visible role models for students, so it is important that they dress professionally and appropriately. There will be some variations in dress according to the different roles and contexts of staff across the trust. The recognition of the Equalities Act 2010 may require the need to deviate from the below and the following can be used as general guidelines:

- Clothing must be professional attire, not casual wear, and worn in a clean and tidy fashion.
- Senior leaders should wear co-ordinated outfits including a jacket
- Male staff must wear a shirt, tie, trousers and shoes.
- Female staff must wear a smart formal top/blouse/dress/skirt/trousers and shoes which may include boots in cold weather and sandals in the summer (subject to health and safety requirements)
- All Technicians/Catering/Premises/Cleaning staff should wear appropriate protective clothing and footwear.
- All staff must wear their name and ID badges.
- In line with the standards for students, staff should not have extreme and un-natural hair colours and styles. The definition of these is at the discretion of the trust.
- Tattoos should be discreetly covered, and the only visible piercings should be to the ear.

The above guidelines are not an exhaustive list and where there is doubt about the suitability of clothing and appearance, the final decision will be made by the school/trust.

Media, Social Media and other forms of Private Publishing and Communication

Any broadcast media contact (newspapers, TV, radio, websites, etc.) must have prior authorisation from the Head of School or other senior staff with a similar or higher status.

Staff should be conscious of not bringing the school/trust into disrepute through their communications on social media and similar channels. This commonly includes inappropriate pictures, negative comments relating to the school/trust, or unprofessional statements or comments which are likely to cause offence or show them in an unprofessional manner and by association bring the school/trust into disrepute.
For this reason, and wherever possible, we would recommend using privacy settings.

Communication between staff and students/parents should be through clear and explicit school systems that set professional boundaries and are always transparent and open to scrutiny. Similarly, staff must not communicate with students or parents through social media or similar, at all times using formal school-based methods of communication. Similarly, staff should not disclose or use their personal telephone numbers, email addresses or similar to contact students or parents.

Mobile Phones

Staff should not use their mobile phone, or other similar devices, during lessons, during staff training, duties or other similar directed time activities. This includes making or receiving calls, texts or email, browsing the internet, playing videos or games, or similar. Any emergency contact should be made via main reception.

Smoking/Alcohol/Drugs/Chewing Gum

Chewing gum, drinking alcohol, using illegal drugs, smoking or vaping are not permitted on trust premises. Staff are expected to report for work in a fit state to carry out their duties in a safe manner; and those found to be under the influence of illegal drugs, alcohol or other substances will be deemed to be unfit for work, and disciplinary action may follow as a consequence.

Conduct Outside Work

Staff must not engage in conduct outside work which could damage their reputation or that of the school/trust. This may be constituted as gross professional misconduct and lead to dismissal.

Use of Staff Cars

Staff must not carry students in their own vehicle unless given permission from appropriate senior staff who will need to be satisfied there is appropriate insurance cover and child protection arrangements are adhered to.

ICT Acceptable Use

The following guidelines apply to staff, students, governors/trustees, volunteers, contractors and visitors. It aims to:

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

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

Users: anyone authorised by the 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 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

Unacceptable use

The following is a non-exhaustive list of what is deemed unacceptable use of school/trust ICT facilities:

- 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 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 brings it into disrepute.

- Sharing confidential information about the school/trust, its pupils, or other members of the school community.
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the 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 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, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school/trust's filtering mechanisms

The trust will use professional judgement to determine whether any act or behaviour not listed is considered unacceptable usage.

Use of Email

Email accounts should be used for work purposes only, and wherever possible all work-related business should be conducted using school/trust email accounts.

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.

If an email is received in error, the sender should be informed, and the email immediately deleted. If the email contains sensitive or confidential information, the user must not make use of that information and maintain its confidentiality and inform a senior member of staff that this has occurred.

Personal use

Staff are permitted to use school ICT facilities for personal use during non-contact/directed time, providing this does not constitute unacceptable use and/or does not interfere or prevent other staff or students from using the facilities for educational purposes Staff may not use the school's ICT facilities to store personal non-work-related information or materials.

Remote access

We allow staff to remotely access ICT facilities and systems. Those doing so must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and take such precautions as they may require from time to time against importing viruses or compromising system security, maintaining data protection and requisite confidentiality.

School Social Media Accounts

Only staff given express permission should access and post on school/trust social media accounts**.**

Monitoring of Network Usage

The trust reserves the right to monitor all aspects of usage relating to ICT facilities and network. It does this for several reasons including checking appropriate and legal usage, quality control, and compliance with legal obligations and requests. Monitoring will be conducted by authorized, suitably qualified staff.

Passwords

All users of the trust's ICT facilities should set robust passwords and keep these passwords private, secure and must not be shared with anyone.

Software Updates, Firewalls, and Anti-Virus Software

Many trust ICT devices have automatic software, security or anti-virus updates. Staff must not circumvent attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

Data Protection

All personal data must be processed and stored in line with data protection regulations and trust data protection policies.

Access to Facilities and Materials

All users of the school's ICT facilities have clearly defined access rights to school/trust systems, files and devices. 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 the Head of School, other senior leader or ICT staff 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 completely at the end of each working day, except for when this enables remote access learning from home or other site.