CARLTON
ACADEMY TRUST

Carlton Academy Trust
Staff Code of Conduct
and ICT Acceptable Use Policy

Approved on behalf of Trustees:	**Gareth Logan**
Approval Date:	**July 2023**
Next Review Date:	**July 2026**

Scope and Policy Aims

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

Glossary

CEO: Trust Chief Executive Officer
COO: Trust Chief Operating Officer
HOS: Head of School
Parents: Umbrella term also including carers

Section One: Appearance and Conduct

Dress and Appearance

Staff act as role models for students, so it is important they dress appropriately and professionally. This will vary according to role and individual circumstances, but following are general guidelines:

- All staff should wear smart, professional clothing appropriate to the role.
- All staff must wear their school/Trust lanyards.
- Staff should not have extreme hair colours or styles.
- Tattoos should be discreetly covered, wherever possible.
- The only visible piercings should be to the ear or a pin to the nose.

These 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 Head of School with delegated authority from the Trust.

Conduct

Alcohol

The consumption of alcohol is not permitted on any Trust site or premises. Anyone found unfit to undertake their duties due to being under the influence of alcohol will be subject to disciplinary action.

Cars

Staff must not carry students in their own vehicle unless given permission from an appropriate senior leader, who will need to ensure there is appropriate insurance cover and child protection arrangements in place.

Chewing Gum

Chewing gum is not permitted on any Trust site or premises.

Contact

Staff must not share or use their personal telephone numbers, email addresses or similar to contact students or parents. All communication must take place through formal school or Trust channels.

Staff must not engage in conduct outside work which could damage their reputation or that of the school/trust. This may lead to disciplinary action.

Dignity at Work

CAT is committed to eliminating harassment and bullying to create a productive working environment where everyone is treated with respect. Harassment and bullying are

unacceptable, and all employees have a duty to behave in a professional and appropriate manner to uphold this standard.

Illegal Drugs

Are not permitted on any Trust site or premises. Anyone found unfit to undertake their duties due to being under the influence of illegal drugs will be subject to disciplinary action.

Media (Mainstream and Social)

Communication with mainstream media sources (newspapers, radio, TV, websites, etc) should be approached with care and caution as comments may lead to significant reputational damage to the school and/or Trust. Therefore, staff must never communicate with mainstream broadcast media sources unless they have express prior authorisation from the HOS l. Before the HOS grants permission, they must also inform and gain approval from the CEO.

Social Media

Staff must take care not to bring the school or Trust into disrepute through their communications on social media. This commonly includes:

- Inappropriate pictures.
- Negative comments about the school or Trust.
- Controversial or negative comments which are likely to cause offence or portray them in an unprofessional manner and by association bring the school or Trust into disrepute.

For these reasons the Trust strongly advises staff to use great discretion when using social media, using privacy settings whenever possible. Staff should never communicate with students or parents through social media, which should always take place through formal school or Trust channels.

Mobile Phones

Staff must not use their mobile phones during lessons, staff training, or other directed time activities. This includes making or receiving calls, texting, sending emails, browsing the internet, playing games or similar. The exception is when an emergency arises.

Smoking and Vaping

Smoking or vaping is not permitted on any Trust site or premises.

Section Two – ICT Acceptable Use

The following guidelines apply to staff, students, governors, members, trustees, volunteers, contractors, and visitors. They aim to:

- Establish rules for the use of school/Trust ICT resources.
- Establish clear expectations for the way Trust staff engage and interact.
- Support Trust policies relating to data protection, online safety, and safeguarding.
- Prevent disruption through misuse or attempted misuse of ICT systems or network.
- Support schools in teaching pupils safe and effective internet and ICT usage.

Definitions

ICT Facilities: Includes all facilities, systems and services including network infrastructure, desktop computers, laptops, tablets, phones, music players, other 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 ICT facilities, including staff, students, governors, Trustees, members, volunteers, contractors, and visitors.

Personal Use: Use or activity not directly related to the users' employment, study or role at the school or Trust.

Authorised Personnel: Staff members authorised by the school to administer or monitor school/Trust ICT systems.

Materials: Files or data created using school/Trust ICT facilities including but not limited to documents, photos, audio, video, printouts, web pages, social networking sites, and blogs.

Unacceptable Use

The following are deemed as unacceptable use of school/Trust ICT facilities:

- Breach of intellectual property rights or copyright.
- Bullying or harassment.
- Promotion or practice of unlawful discrimination.
- Breaching school/Trust policies or procedures.
- Illegal conduct or promotion of illegal conduct.
- 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 brings it into disrepute.
- Sharing confidential information about the school/Trust, its students, or other members of the school/Trust community.
- Connecting any non-school/Trust device to the Trust network without approval from authorised personnel.
- Setting up software, applications, or web services on the Trust network without approval from authorised personnel.
- Creating or using any program, tool or item of software designed to interfere with the functioning of the Trust network, ICT facilities, accounts, or data.
- Gaining or attempting to gain access to restricted areas of the network, or password protected information without approval from authorised personnel.

- Allowing, encouraging, or enabling others to gain or attempt to gain unauthorised access to Trust/school ICT facilities.
- Causing intentional damage to ICT facilities
- Removing, deleting, or disposing of ICT equipment, systems, programs, or information without permission from authorised personnel.
- Creating a data breach by accessing, modifying, or sharing data to which a user is not supposed to have access or without proper authorisation.
- Using inappropriate or offensive language.
- Promoting a private business, except where a direct subsidiary of the school/Trust.
- Using websites or mechanisms to bypass the school/Trust filtering mechanisms.

The school/Trust will use professional judgement to decide whether any other circumstance is considered unacceptable usage.

Email

School/Trust 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 email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or similar.

Where an email is received in error, the sender should be informed, and the message immediately deleted. When it contains sensitive or confidential information, the receiver must not make use of the information, maintain confidentiality, and inform an appropriate senior leader without delay.

Use of USB Memory Sticks and Flash Drives

USB memory sticks and flash drives **must not** be used on Trust ICT facilities as their use threatens and compromises cybersecurity of the Trust network.

Personal use

Staff are permitted to use school/Trust ICT facilities for personal use during non-directed time providing this does not constitute unacceptable use and does not interfere or prevent others from using school/Trust ICT facilities. Staff may not use school/Trust ICT facilities to store personal information.

Remote access

Those remotely accessing Trust networks must abide by the same rules as those accessing the network on-site, paying attention and vigilance to ensure they don't import viruses, compromise cybersecurity, and maintain standards of confidentiality and data protection.

School Social Media Accounts

Only staff with express permission and access rights should access and post on school/Trust social media accounts**.**

Monitoring Network Usage

The Trust reserves the right to check all aspects of ICT network and facility usage. This is completed by Trust personnel and our outsourced network providers.

Passwords

All network users must set robust passwords in accordance with Trust guidelines, kept private, secure, and not shared with anyone.

Software Updates, Firewalls, and Anti-Virus Software

Staff must not circumvent or attempt to circumvent software updates (including anti-virus) firewalls, or any other system to protect Trust networks and ICT facilities.

Data Protection

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

Access to Facilities and Materials

All users have clearly defined access rights to Trust networks, software, files, and devices. They must not access or attempt to access systems, files, or devices to which they have not been granted access.

Where access is provided in error, or if something is shared in error, they should alert the HOS or COO without delay.

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