
# Staff & Volunteer ICT Acceptable Use Policy

| | |
|---|---|
| Document Owner: | Director of IT Services |
| Version | 1.0 |
| Document Status: | Approved |
| Classification: | External |
| Review Date: | 01/04/19 |
| Effective from: | 01/04/17 |

# Table of Contents



# Policy Introduction

The internet and other technologies are powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have and entitlement to good, safe access to ICT and the internet. This Acceptable Use Policy is intended not to restrict legitimate and authorised activity but to ensure that:

- Staff and volunteers are responsible users and stay safe while using technologies for educational, personal and recreational use.
- School ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Staff and volunteers are protected from potential risk from the use of ICT in their everyday work and work to ensure that young people in their care are safe users.

# General Computer Use

When using the Trust's ICT equipment and other information systems, I have understood and will comply with the following statements:

- I have read and understood the implications and my personal responsibilities in relation to the use of ICT equipment which is detailed within this policy.

- I will access the internet and other ICT systems using an individual username and password, which I will keep secure. I will ensure that I log out after each session and never allow other users to access the internet through my user name and password. I will report any suspicion, or evidence that there has been a breach of my personal security in relation to access to the internet or ICT systems.

- All passwords I create will be in accordance with the academies password policy. I will ensure that I use a suitably complex password for access to the internet and ICT systems and that I will use a unique password for each system.

- I will not share my passwords with any colleagues or pupils.

- I will seek consent from the IT Department prior to the use of any new techniques (hardware, software, cloud-based services).

- I will not search for, download, upload or forward any content that is illegal or that could be considered an offence by another user. If I encounter any such material I will report it immediately to the IT Department.

- I will take a professional and proactive approach to assessing the effectiveness of the internet content-filtering platform in relation to the educational content that can be viewed by the pupils in my care.

- I will not attempt to bypass any filtering and/or security systems put in place. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the IT Department.

- I will ensure that data stored on devices taken off site, (laptops, tablets, cameras, removable media, and phones) will be secured in accordance with TAG Data Protection Policy and any information-handling procedures both on and off site.

- I understand my personal responsibilities in relation to the Data Protection Act and the privacy and disclosure of personal and sensitive confidential information.

- I will take reasonable precautions to ensure that any devices (laptops, tablets, camera, removable media or phones) are stored in a secure manner when taken off site (car/home/other location). Devices will not be stored in a car overnight or left in sight when not in use, e.g. by an open window or on the back seat of a car.

- I will secure any equipment taken off site for school trips.

- I will ensure that any personal or sensitive information taken off site will be situated on a TAG-owned device with appropriate technical controls such as encryption/password protection deployed.

- Any information asset, which I create from other information systems, which could be deemed as personal or sensitive will be stored on the network and access controlled in a suitable manner in accordance with the data protection controls. (For example spreadsheets/other documents created from information located within the SIMS).

- I will not download or install any software from the internet or from any other media which may compromise the network or information situated on it without prior authorization.

- I will return any TAG-owned ICT equipment or software directly to the IT Department once it is no longer required.

- I understand that my files, communications and internet activity may be monitored and checked at all times to protect my own and others' safety, and action may be taken of deemed necessary to safeguard me or others.

- I understand that if I do not follow all statements in this AUP and in other policies relating to the use of ICT equipment I may be subject to disciplinary action in line with the established procedures.

## Social Media

- I must not talk about my professional role in any capacity when using personal social media such as Facebook, Twitter and YouTube or any other online publishing. Reposting information already online is allowed.

- I must not use social media tools to communicate with current or former pupils under the age of 18 unless approved in writing by the Head Teacher.

- I will not use any social media tools to communicate with individual parents regarding students unless approved in writing by the Head Teacher.

- I will set and maintain my profile on social networking sites to maximum privacy and give access to known friends only.

## Managing digital content

- I will demonstrate professional, safe and responsible behaviour when creating, using and storing digital images, video and sound.

- I will only use Trust owned equipment to create digital images, videos and sound. Digital images and video will be of appropriate activities and participants will be in appropriate dress. No resources will be published online without the permission of the staff and pupils involved as detailed in the eSafeguarding Policy (or any other relevant policy).

- Under no circumstances will I use any personally-owned equipment for video, sound or images without prior consent from the designated member of staff.

- When searching for images, video or sound clips, I will ensure that I or any pupils in my care are not in breach of any copyright law.

- I will ensure that any images, videos or sound clips or pupils are stored on the network and never transferred to personally-owned equipment.

- I will ensure that any images taken on TAG owned devices will be transferred to the network (storage area/server) and immediately deleted from the memory card.

- I will model safe and responsible behaviour in the creation and publishing of online content with the VLE platform and any other websites. In addition to this I will encourage colleagues and pupil to adopt similar safe behaviour in their personal use of blogs, wikis and online publishing sites.

## Teaching and Learning

- I will support and promote the eSafeguarding policy at all times. I will model safe and responsible behaviour in pupils when using ICT to support teaching and learning.

- I will ensure that I am aware of my individual responsibilities relating to the safeguarding of children within the context of eSafeguarding and know what to do in the event of misuse of technology.

- I understand the importance of respecting and acknowledging copyright of materials found on the internet and will model best practice in the creation of my own resources at all times.

## Email

- I will use my academy email address for all correspondence with staff, parents or other agencies and I understand that any use of the academy email system will be monitored and checked. I will under no circumstances use my private email account for any academy-related business.

- Communication between staff and pupils or members of the wider academy community should be professional and related to academy matters only.

- I will ensure that any posts made on websites or via electronic communication, by either myself or the pupils in my care, will not damage the reputation of academy/Trust.

- I will not synchronize any academy email account with a personally-owned handheld device unless approved by the IT department.

- I will take care in opening any attachments sent by email. I will only open emails and associated attachments from trusted senders.

- Emails sent to external organizations will be written carefully. As and when I feel it necessary, I will carbon copy (cc) your, line manager or another suitable member of staff into the email.

- I will ensure that I manage my email account; delete unwanted emails and file those I need to keep in subject folders.

- I will access my academy email account on a regular basis to ensure that I respond in a timely manner to communications that require my attention.

## Mobile phones and devices

- I will not make/receive calls/texts on my personal phone during contact time with students. Emergency contact should be made via the main office.

- I will set my phone to silent or switch off during contact with students.

- Bluetooth communication will be switched off and mobile phones or devices e.g. Smart watches will not be used during contact with students unless permission has been granted by a member of Senior Leadership Team in emergency circumstances.

- I will not use any personally-owned mobile device to take images, video or sound recordings of students.

- Should there be exceptional circumstances (e.g. acutely sick relative), then staff or volunteer must make the Head Teacher aware of this and can have their phone in case of having to receive an emergency call.

# Appendix A: LEGISLATION & REGULATIONS

This policy respects and complies with the applicable laws including (but not limited to):

- Telecommunications Act 1984
- Copyright, Designs & Patents Act 1988
- Computer Misuse Act 1990
- Disability Discrimination Acts & SENDA 1995
- Data Protection Act 1998
- Human Rights Act 1998
- Regulation of Investigator Powers Act 2000
- Freedom of Information Act 2000
- Electronic Communications Act 2000
- Copyright (Computer Software) Amendment Act (1985) and The Copyright (Computer Programs) Regulations 1992
- Health and Safety (Display Screen Equipment) Regulations 1992 (amended 2002)
- Child Exploitation and Online Protection (CEOP)

# Agreement

I have read and understand all of the TAG Staff and Volunteer Acceptable Use Policy relating to my use of technology. I understand that if I fail to comply with this Acceptable Use Policy agreement, I could be subject to disciplinary action.

| | |
|---|---|
| **Staff Name** | |
| **Signed** | |
| **Date** | |