

## ICT Acceptable Use Policy

### SCOPE

*As a professional organisation with responsibility for children's safeguarding, it is important that all staff within the organisation take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse, and theft.*

*All members of staff have a responsibility to use the organisation's computer system in a professional, lawful, and ethical manner.*

*To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the Academy systems, they are asked to read and sign this ICT Acceptable Use Policy.*

### **By signing this ICT Acceptable Use Policy, you are agreeing to the following terms:**

- I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies, and access devices. Examples include mobile phones, PDAs, digital cameras, email, and social media sites.
- Academy-owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences; or to modify computer material without authorisation.
- I understand that any hardware and software provided by the Academy for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate. Equipment provided by the Academy is only to be used by employees and not by members of their family.
- I will respect system security and will not disclose any password or security information to anyone. I will use a 'strong' password (a strong password has numbers, letters, and symbols, with six or more characters and is only used on one system).
- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the Technical Services Team.

### **Legislation Compliance**

- I will ensure that any personal data of pupils, staff, or parents/carers is processed in accordance with the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR). This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary, and kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls), or accessed remotely.
- Any data which is being removed from Young Technicians Academy (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the Academy. Any images or videos of pupils will only be used as stated in the Academy's image use policy and will

always consider parental consent. If I am given an encrypted device to safely transport data off-site, I will not leave it in an unencrypted state.

### **Data Security**

- I will not keep professional documents that contain Academy-related sensitive or personal information (including images, files, videos, etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are secured and encrypted. Where possible, I will only upload work documents and files to Academy-approved cloud platforms that comply with UK GDPR requirements and use secure encryption protocols.
- I will protect the devices in my care by ensuring they are password-protected, have regular software updates, and are equipped with up-to-date antivirus software to prevent unauthorised access or theft.
- I will not store any personal information on the Academy's computer system that is unrelated to Academy activities, such as personal photographs, files, or financial information. I will respect copyright and intellectual property rights.

### **E-Safety and Safeguarding**

- I have read and understood the Academy's E-Safety Policy, which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites, and the supervision of pupils within the classroom and other working spaces.
- I will promote e-Safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use, and the content they access or create.
- I will report all incidents of concern regarding children's online safety to the Designated Safeguarding Lead (DSL) as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches, or unsuitable websites to the E-Safety Coordinator.
- I will not attempt to bypass any filtering and/or security systems put in place by the IT department. If I suspect a computer or system has been damaged or affected by a virus or other malware, or if I have lost any Academy-related documents or files, I will report this to ICT Support as soon as possible.

### **Communication and Usage Guidelines**

- Electronic communications with students, parents/carers, and other professionals will only take place via work-approved communication channels, e.g., via an organisation-provided email address or telephone number. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership Team.
- My use of ICT and information systems will always be compatible with my professional role, whether using Academy or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications, and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the organisation's AUP and the Law.
- I will not create, transmit, display, publish, or forward any material that is likely to harass, cause offence, inconvenience, or needless anxiety to any other person, or anything which could bring my professional role or the Academy into disrepute.

## Cybersecurity Awareness

- I will complete any cybersecurity awareness training provided by the Academy to help identify and respond to potential threats, such as phishing or malware attacks.
- I understand that irrespective of the location and circumstance, my use of the organisation's IT systems (including the Internet and email) may be monitored and recorded to ensure policy compliance.
- The organisation may exercise its right to monitor the use of information systems, including Internet access and the interception of emails, to ensure compliance with this Acceptable Use Policy. Where it believes unauthorised and/or inappropriate use of the organisation's systems or unacceptable/inappropriate behaviour may be taking place, the Academy will invoke its disciplinary procedure. If it is suspected that the system may be being used for criminal purposes or for storing unlawful text, imagery, or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

## Agreement

*By signing this ICT Acceptable Use Policy, you are agreeing to the terms outlined above.*

Employee Full Name: .....

Position: .....

Date: .....

Sign: .....