ACCEPTABLE USE OF ICT POLICY

1. Introduction and aims

Information and communications technology (ICT) is an integral part of the way Train'd Up operates, and is a critical resource for learners, staff (including senior leadership teams), members of the governance board and visitors. It supports teaching and learning, pastoral and administrative functions of each Team / Department.

However, the ICT resources and facilities Train'd Up uses also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of Train'd Up ICT resources for staff, learners, and members of the governance board
- Establish clear expectations for the way all members of Train'd Up's community engage with each other online
- Support Train'd Up's policies on data protection and safeguarding
- Prevent disruption to Train'd Up through the misuse, or attempted misuse, of ICT systems
- Support Train'd Up in teaching learners safe and effective internet and ICT use
- This policy covers all users of Train'd Up's ICT facilities
- Breaches of this policy may be dealt with under our Disciplinary Policy.

2. Relevant legislation and guidance

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

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Freedom of Information Act 2000
- Keeping Children Safe in Education 2023
- Education and Training (Welfare of Children) Act 2021

3. Definitions

- **ICT facilities:** includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, 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 Train'd Up ICT service
- **Users:** anyone authorised by Train'd Up to use the ICT facilities, including members of the governance board, staff, learners, contractors and visitors
- **Personal use:** any use or activity not directly related to the users' employment, study or purpose
- **Authorised personnel:** employees authorised by Train'd Up 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
  See appendix 3 for a glossary of cyber security terminology.

4. Unacceptable use

The following is considered unacceptable use of Train'd Up's ICT facilities by any member of the Train'd Up community. Any breach of this policy may result in disciplinary proceedings (see section 4.2 below).

Unacceptable use of Train'd Up's ICT facilities includes:

- Using Train'd Up's ICT facilities to breach intellectual property rights or copyright
- Using Train'd Up's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching Train'd Up's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting)
- Activity which defames or disparages Train'd Up, or risks bringing the company into disrepute
- Sharing confidential information about Train'd Up, its learners, or other members of the Train'd Up community
- Connecting any device to Train'd Up's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on Train'd Up's 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 Train'd Up's 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 Train'd Up
- Using websites or mechanisms to bypass Train'd Up's filtering mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic or discriminatory in any other way
- Using AI tools and generative chatbots (such as ChatGPT and Google Bard):
    - During assessments, including internal and external assessments, and coursework
    - To write their work / assignments, where AI-generated text or imagery is presented as their own work

This is not an exhaustive list. Train'd Up reserves the right to amend this list at any time. The Managing Director will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of Train'd Up's ICT facilities.

4.1 Exceptions from unacceptable use

Where the use of Train'd Up ICT facilities (on Train'd Up premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Managing Director's discretion.

Learners may use AI tools and generative chatbots:

- As a research tool to help them find out about new topics and ideas
- When specifically studying and discussing AI in studies, for example in IT related lessons or engineering assignments about AI-generated images. All AI-generated content must be properly attributed

4.2 Sanctions
Learners and staff who engage in any of the unacceptable activity listed above may face disciplinary action.

5. STAFF (INCLUDING MEMBERS OF THE GOVERNANCE BOARD AND CONTRACTORS)
Access to Train'd Up ICT facilities and materials
Train'd Up's IT Technical Support Team (Central UK) manages access to Train'd Up's ICT facilities and materials for Train'd Up staff, that includes, but is not limited to:

- Computers, tablets, mobile phones and other devices
- Access permissions for certain programmes or files
- Staff will be provided with unique log-in/account information and passwords that they must use when accessing Train'd Up's ICT facilities. Logins/access to Train'd Up's network must go via the IT Technical Support Team (Central UK)
- Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the IT Technical Support Team (Central UK)

5.1 Use of phones and email
- Train'd Up provides each member of staff with an email address, this email account should be used for work purposes only.
- All work-related business should be conducted using the email address Train'd Up has provided.
- Staff must not share their personal email addresses with learners, parents / guardians and must not send any work-related materials using 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 attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient. To send a secure email add the word 'SECURE' to the start of the email subject.
- 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 that contains the personal information of another person, they must inform the Managing Director immediately and follow data breach procedures.
- Staff must not give their personal phone numbers to learners or parents / guardians. Staff must use phones provided by Train'd Up to conduct all work-related business.
- Train'd Up 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.

5.2 Personal use
Staff are permitted to occasionally use Train'd Up ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Managing Director may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during contact time/teaching hours/non-break time.
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no learners are present
- Does not interfere with their jobs, or prevent other staff or learners from using the facilities for work or educational purposes
- Staff may not use Train'd Up's ICT facilities to store personal non-work-related information or

materials (such as music, videos or photos).
- Staff should be aware that use of Train'd Up's ICT facilities for personal use may put personal communications within the scope of Train'd Up's ICT monitoring activities (see section 5.6). Where breaches of this policy are found, disciplinary action may be taken.
- Staff should be aware that personal use of ICT (even when not using Train'd Up ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where learners and parents / guardians could see them.
- Staff should take care to follow Train'd Up's guidelines on social media (see appendix 1) and use of phones and email (see section 5.1) to protect themselves online and avoid compromising their professional integrity.

5.3 Personal social media accounts
Members of staff should ensure their use of social media, either for work or personal purposes, is always appropriate.

5.4 Remote access
Staff accessing Train'd Up's 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 Train'd Up's ICT facilities outside the company and take such precautions as the IT Technical Support Team (Central UK) may require from time to time, against importing viruses or compromising system 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.

5.5 Train'd Up social media accounts
The Train'd Up has an official Facebook and Twitter page, managed by the Quality & Compliance Team. Staff members who have not been authorised to manage, or post to, the account; must not access, or attempt to access the account. These are the only social media accounts accepted by Train'd Up and requests for additional pages/sites must be approved directly by the Managing Director.

The Train'd Up 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 always abide by these guidelines.

5.6 Monitoring and filtering of Train'd Up network and use of ICT facilities
To safeguard and promote the welfare of users of our facilities and provide them with a safe environment to learn, Train'd Up reserves the right to filter and monitor the use of its ICT facilities and network.

This includes, but is not limited to, the filtering and monitoring of:
- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised ICT staff may filter, inspect, monitor, intercept, assess, record, and disclose the above, to the extent permitted by law.

Train'd Up monitors ICT use in order to:
- Obtain information related to Train'd Up business
- Investigate compliance with Train'd Up policies, procedures, and standards
- Ensure effective Train'd Up 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

The Train'd Up Governance Board is responsible for making sure that:

- Train'd Up and its Team / Departments meets the DfE's filtering and monitoring standards
- Appropriate filtering and monitoring systems are in place
- Staff are aware of those systems and trained in their related roles and responsibilities
- For the leadership teams and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns
- It regularly reviews the effectiveness of the Team / Department's monitoring and filtering systems

The Managing Director, supported by the IT Technical Support Team (Central UK) will take lead responsibility for understanding the filtering and monitoring systems and processes in place.

Where appropriate, staff may raise concerns about monitored activity with a DSL and the IT Technical Support Team (Central UK), as appropriate.

6. LEARNERS

6.1 Unacceptable use of Train'd Up ICT equipment out with Train'd Up premises

Any learner found to be engaging in any of the following **at any time** (even if they are not on Train'd Up premises) will be subject to disciplinary action:

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching Train'd Up'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
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages Train'd Up, or risks bringing Train'd Up into disrepute
- Sharing confidential information about Train'd Up, other learners, or other members of Train'd Up community
- 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 Train'd Up's ICT facilities
- Causing intentional damage to ICT facilities or materials
- 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

7. Data security

Train'd Up is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and learners. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cyber-crime technologies.

Staff, learners, parents / guardians and others who use Train'd Up's ICT resources should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education's guidance on digital and technology standards in Team / Departments and colleges, including the use of:

- Firewalls
- Security features
- User authentication and multi-factor authentication
- Anti-malware software

7.1 Passwords

All users of Train'd Up's 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 learners who disclose account or password information may face disciplinary action.

User passwords are generated based on secret information only known to the user. On first login these are then reset to a secure password – minimum 12 characters, a capital letter, a lower-case letter, a number and a special character. All must not contain the user's name. Only the IT Technical Support Team (Central UK) can reset passwords.

7.2 Software updates, firewalls, and anti-virus software

All Train'd Up's 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 Train'd Up's ICT facilities.

Any personal devices using Train'd Up's network must all be configured in this way.

7.3 Data protection

All personal data must be processed and stored in line with data protection regulations and Train'd Up's Data Protection Policy.

7.4 Access to facilities and materials

All users of Train'd Up's ICT facilities will have clearly defined access rights to Train'd Up systems, files and devices.

These access rights are managed by the IT Technical Support Team (Central UK).

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 IT Technical Support Team (Central UK) 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.

7.5 Encryption

The Train'd Up ensures that its devices and systems have an appropriate level of encryption.

Train'd Up staff may only use personal devices (including computers and USB drives) to access Train'd Up data, work remotely, or take personal data (such as learner information) out of Train'd Up if they have been specifically authorised to do so by the Managing Director.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the technical services team.

7.6 Protection from cyber attacks

Please see the glossary (appendix 3) to help you understand cyber security terminology.

Train'd Up will:

- Work with the IT Technical Support Team (Central UK) to make sure cyber security is given the time and resources it needs to make Train'd Up secure
- Provide training for staff and include this training in any induction for new starters on the basics of cyber security, including how to:
    - Check the sender address in an email
    - Respond to a request for bank details, personal information or login details

    - Verify requests for payments or changes to information
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Put controls in place that are:
    - **'Proportionate'**: Train'd Up will verify this using a third-party audit (such as 360 degree safe) 6 monthly, to objectively test that what it has in place is up to scratch
    - **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
    - **Up to date:** with a system in place to monitor when Train'd Up needs to update its software
    - **Regularly reviewed and tested**: to make sure the systems are as up to scratch and secure as they can be
- Backup critical data daily, every night to a backup NAS.
- Delegate specific responsibility for maintaining the security of our management information system (MIS)
- Make sure staff where possible:
    - Enable multi-factor authentication where they can, on things like Train'd Up email accounts
    - Store passwords securely using a password manager
- Make sure ICT staff conduct regular access reviews to make sure each user in Train'd Up has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Check that its supply chain is secure, for example by asking sub-contractors about how secure their business practices are and seeing if they have the Cyber Essentials certification
- Develop, review and test an incident response plan with the IT Technical Support Team (Central UK), for example, including how Train'd Up will communicate with everyone if communications go down, who will be contacted when, and who will notify Action Fraud of the incident. This will be reviewed and tested every 6 month and after a significant event has occurred, using the NCSC's 'Exercise in a Box'

8. Internet access

- Train'd Up internet connection is secured
- Train'd Up internet access is designed for learners and includes a filtering system to prevent access to inappropriate sites
- Staff will check that the sites pre-selected for learner use are appropriate
- Staff will be particularly vigilant when learners are undertaking their own search and will check that learners are following an agreed search plan
- We have filtering running on our firewall, reinforced by both SmoothWall and Senso filtering. These are monitored proactively by the IT Technical Support Team (Central UK). Alerts are also sent to DSLs and line managers when necessary. Any monitored sites that are not caught initially with filtering are added manually to the blacklist.

9. Monitoring and review

The Managing Director and the IT Technical Support Team (Central UK) monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of Train'd Up. This policy will be reviewed every year, the Managing Director and the IT Technical Support Team (Central UK) are responsible for approving this policy.

10. Related policies

This policy should be read alongside the following Train'd Up's policies / procedures:

- Risk Management Policy
- Quality Improvement Policy
- Plagiarism Policy
- Safeguarding Policy
- Prevent Policy
- Disciplinary & Grievance Procedures (staff)
- Data Protection Policy GDPR
- Mobile Phone Policy

11. Director Policy Approval

This Policy is reviewed as a minimum on an annual basis and is approved and endorsed by the Board of Directors, Senior Management Team.

Signed on behalf of Company Directors:

Name: Alan Wilson
Position: Managing Director
Date: 12/08/2024

Appendix 1: ACCEPTABLE USE AGREEMENT FOR LEARNERS

Acceptable use of Train'd Up's ICT facilities and internet: agreement for learners	
Name of learner:	
When using Train'd Up's ICT equipment and accessing the internet in Train'd Up, I will not: • Use them for a non-educational purpose • Use them without a tutor / assessor being present, or without a tutor / assessor's permission • Use them to break Train'd Up rules • Access any inappropriate websites • Access social networking sites (unless my tutor / assessor has expressly allowed this as part of a learning activity) • Use chat rooms • Open any attachments in emails, or follow any links in emails, without first checking with a tutor / assessor • Use any inappropriate language when communicating online, including in emails • Share any semi-nude or nude images, videos or livestreams, even if I have the consent of the person or people in the photo • Share my password with others or log in to Train'd Up's network using someone else's details • Bully other people I understand that if issued with a laptop, or other IT equipment for study purposes, I am not to lend any IT equipment to anyone, including members of my family, for any reason. I understand that I am expected to protect loaned IT equipment from damage and theft, and that I will be responsible for damage or theft that takes place off Train'd Up premises. I understand that it is my responsibility to ensure the safe return of any issued IT equipment direct to my assessor / trainer, on leaving early or completing studies. Failure to do will result in an invoice being raised to the value of replacement IT equipment. All IT equipment must be returned within 14 days of leaving or completing studies. I understand that I will **not** be held responsible for IT equipment problems resulting from regular study related use, however, I will be held responsible for any problems caused by negligence, as assessed by the IT Technical Support Team (Central UK). I understand that Train'd Up will monitor the websites I visit and my use of Train'd Up's ICT facilities and systems. I will immediately inform a member of Train'd Up, if I find any material which might upset, distress or harm me or others. I will always use Train'd Up's ICT facilities systems and internet responsibly. I understand that I may be subject to disciplinary action if I undertake unacceptable activities online, whilst using IT facilities and accessing the internet.	
Signed (learner):	**Date:**

Appendix 2: ACCEPTABLE USE AGREEMENT FOR STAFF, GOVERNANCE BOARD

Acceptable use of Train'd Up's ICT resources, facilities and internet: agreement for staff and governance board	
Name of staff member/governor:	
When using Train'd Up's ICT resources, facilities and accessing the internet in Train'd Up, or outside Train'd Up on a work device, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm Train'd Up's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to Train'd Up's network • Share my password with others or log in to Train'd Up's network using someone else's details • Share confidential information about Train'd Up, its learners or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to Train'd Up	
I understand that I am not to lend my company laptop (or any other IT equipment) to anyone, including members of my family, for any reason. I understand that I am expected to protect my laptop (or any other IT equipment) from damage and theft, and that I will be responsible for damage or theft that takes place off company premises. I understand that I will **not** be held responsible for IT problems resulting from regular business-related use, however I will be held responsible for any problems caused by my negligence, as assessed by the IT Technical Support Team (Central UK). I understand that, if I leave the company, I must return my laptop (or any other IT equipment) to: Head of Finance, Train'd Up, Old Manor House, 129 Henderson Street, Bridge of Allan, FK9 4RQ. I understand that Train'd Up will monitor the websites I visit and my use of Train'd Up's ICT resources, facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password protected when using them, and keep all data securely stored in accordance with this policy and Train'd Up's Data Protection Policy GDPR. I will inform the designated safeguarding lead (DSL) and IT Technical Support Team (Central UK) if a learner informs me, they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use Train'd Up's ICT systems and internet responsibly and ensure that learners I am responsible for also do.	
Signed:	**Date:**

Appendix 3: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber-attack and the measures Train'd Up will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Breach	When your data, systems or networks are accessed or changed in a non-authorised way.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.

Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.

TERM	DEFINITION
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programmes designed to self-replicate and infect legitimate software programs or systems.
Virtual private network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly-targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.