INFORMATION TECHNOLOGY AND SOCIAL MEDIA POLICY & PROCEDURE – LEARNER AND EMPLOYER

1. **Purpose**
    a) This policy may be updated from time to time, to comply with legal and policy requirements. It is intended to provide a framework for the use of Information Technology (I.T.) resources and personal social media by ETT learners. It should be interpreted such that it has the widest application and to include new and developing technologies and uses, which may not be explicitly referred to.
2. **Scope**
    a) ETT seeks to promote and facilitate the positive and extensive use of IT in the interests of supporting the setting up and delivery of learning to the highest possible standards.
    b) This also requires appropriate and legal use of the technologies and facilities made available to learners and employers.
3. **Definitions**
    a) **Learner:** An ETT Apprentice or learner who has access to OneFile and/or attends The Engineering Skills Academy (TESA) or a subcontractor.
    b) **Employer:** A person who represents a company whose staff are Learners. An Employer may refer to several people at a company who are part of the Learner's apprenticeship delivery such as a manager or mentor.
    c) **IT Equipment:** Electronic devices owned and controlled by ETT.
    d) **IT Platform:** Technologies and tools that support the development, deployment, management, and operation of digital services, or systems used to operate our business and deliver our services.
    e) **Personal Device:** An electronic device not owned/controlled by ETT.
    f) **ETT Network:** The infrastructure provided by ETT at TESA including internet connection, cabling, and servers.
    g) **Social Media:** There are more than 200 well-established social media platforms globally; however, the most popular in the UK and relevant to our policy include: YouTube, Instagram/Threads, TikTok, Snapchat, WhatsApp, Discord, Reddit, Be Real, Pinterest, X (formerly Twitter), BlueSky, LinkedIn, Telegram, Twitch, and Kick. These platforms represent the primary channels for video sharing, networking, messaging, and live streaming. ETT recognises that emerging platforms may gain popularity, and this list is reviewed annually to ensure relevance.
    h) **Personal Social Media Account:** A social media profile used primarily for personal, non-professional purposes, including private messaging functions.
4. **Roles and Responsibilities**
    a) Learners and Employers are responsible for adhering to the acceptable use policies outlined in this document, safeguarding their own authentication credentials, and reporting any security concerns or incidents as defined in Section 9.
    b) The Designated Safeguarding Lead (DSL) is responsible for assessing and acting upon any safeguarding concerns arising from IT or social media use, in line with the separate Safeguarding and Prevent policies.

c) The Chief Executive (or delegated nominee) is responsible for the overall governance of IT, ensuring appropriate resources are allocated for IT security, and managing the relationship with external IT providers.
d) The External IT Support Provider is responsible for the technical implementation, configuration, monitoring, and maintenance of all IT Equipment, IT Platforms, and the ETT Network in accordance with industry best practice and the requirements implied by this policy.

5. IT Unacceptable Use

a) IT Equipment, IT Platforms, and the ETT Network may not be used directly or indirectly by a Learner or Employer for the download, creation, manipulation, transmission, or storage of:
   i. any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material
   ii. unlawful material, or material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalise themselves or others
   iii. unsolicited "nuisance" emails
   iv. material which is subsequently used to facilitate harassment, bullying and/or victimisation of a member of ETT staff, Learner or third party
   v. material which promotes discrimination based on race, gender, religion or belief, disability, age, or sexual orientation
   vi. material with the intent to defraud or which is likely to deceive a third party
   vii. material which advocates or promotes any unlawful act
   viii. material that infringes the intellectual property rights or privacy rights of a third party, or that is in breach of a legal duty owed to another party, or
   ix. material that brings ETT into disrepute.
   x. Uploading ETT data into public AI tools is prohibited unless approved in accordance with the Section 6 - External Platforms & Data Handling
b) IT Equipment, IT Platforms, and the ETT Network may not be used directly or indirectly by a Learner or Employer for activities having, or likely to have, any of the following characteristics:
   i. Intentionally wasting effort or other ETT resources
   ii. Corrupting, altering, or destroying another Learner's data without their consent
   iii. Disrupting the work of other Learners
   iv. Denying access to other Learners
   v. Pursuance of commercial activities outside of those in support of learning activities
c) Where IT Equipment is being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use under this policy. Learners shall not:
   i. introduce data-interception, password-detecting or similar software or devices to the ETT IT Equipment, IT Platforms, and the ETT Network,
   ii. seek to gain unauthorised access to restricted areas of the ETT Network,
   iii. access or try to access data where the user knows or ought to know that they should have no access,
   iv. carry out any hacking activities,

v. intentionally or recklessly introduce any form of spyware, computer virus, or other potentially malicious software, or
vi. add ETT data to an un-authorised cloud service without the permission of the Chief Executive.

6. External Platforms & Data Handling

a) ETT data must not be uploaded, processed, stored, or entered into any external platform, service, or tool unless that platform has been formally approved by ETT and explicit written permission has been granted by the Chief Executive.
b) Platforms covered by this rule include, but are not limited to public or consumer grade Artificial Intelligence tools (e.g. ChatGPT, Google Bard, Microsoft Copilot etc)
c) This requirement protects ETT from data breaches, loss of control, non-compliance with GDPR, and exposure to insecure or unregulated services.
d) Users must obtain explicit written approval from the Chief Executive before uploading any ETT data into an external service.
e) Data protection and GDPR compliance, including learner rights of access and rectification, are covered in a separate Data Protection Policy. Learners and employers should refer to that policy for details on how their personal data is handled.

7. PINs, Passwords, MFA, and Electronic Signatures

a) **Principles**
i. Always keep passwords and PINs safe and secure
ii. Do not allow another Learner or Employer to use IT Equipment or an IT Platform that is logged in under your name. It is your responsibility to ensure other Learners or Employers cannot access IT Equipment or an IT Platform under your name.
iii. Do not use any ID which is not your own or use a piece of IT Equipment or IT Platform which is logged in under an ID which is not yours, unless authorised to do so by the Chief Executive.
iv. Individuals must not request, record, store, share, or handle any ETT staff, Learner or Employer PINs, Passwords, or Electronic Signature credentials. These are personal authentication identifiers and must remain confidential to the individual they belong to.

b) **PIN:** A four-digit code specific to an individual ETT staff member, Learner, or Employer (individuals under 'Employer' would have unique codes) used to digitally sign documents related to a Learner's apprenticeship within the ETT LMS platform.
i. PINs act as secure digital confirmation that an individual named in a document or process has confirmed their understanding and agreement. If an ETT staff member, Learner, or Employer knowingly uses another person's PIN, the authenticity of the confirmation is compromised, and the verification that the correct individual authorised the document is impossible.
ii. ETT staff members, Learners, and Employers must not use a PIN to electronically sign documents, reviews, declarations, or compliance related information on behalf of another person. To do so is deemed as misconduct and the appropriate ETT Policy and Procedure will be used to address the issue.
iii. Our Apprentice Review Portal (ARP) automatically applies an accurate date and time stamp when users enter their own PIN. A time or date stamp

becomes misleading and invalidates the audit trail if not completed by the authorised person.

c) **Password:** A secret piece of information, usually a string of letters, numbers, and symbols, that an individual must provide to gain access to IT Equipment, IT Platform or ETT Network.
   i. Learners and Employers must create a password that is not a name or a complete word, nor a common abbreviation. A combination of ten (or more) letters/numbers/symbols is recommended with a mix of capital and lower-case letters.
   ii. Learners and Employers should change their password regularly (you will periodically be prompted to do so by some platforms). Avoid writing down your password.
   iii. Passwords act as secure digital confirmation that an authorised individual is accessing IT Equipment, an IT Platform or ETT Network. If a Learner or Employer knowingly uses another person's Password it reduces the security and integrity of that equipment, platform, or network.

d) **Electronic Signatures:** An electronic method of indicating agreement or approval of a document.
   i. Learners and Employers may be asked to sign documents using an Electronic Signature.
   ii. Signer identity confirmation through a recognised email address previously provided by the individual.
   iii. We accept typed, drawn, and digital signatures within the SignNow platform.

8. Compliance & Professional Standards

a) Apprenticeship and organisational documentation must comply with funding rules, Ofsted expectations, external audit standards, and internal quality processes.
b) Ensuring that only the appropriate individual uses their own authentication details supports transparency, professional conduct, and a secure and accountable digital environment.

9. Reporting Concerns

a) Misuse of PINs, passwords, or electronic signatures, whether involving an ETT staff member, Learner or Employer, must be reported immediately.
b) Concerns should be reported directly to either:
   i. The CEO, or
   ii. The Director of Delivery and Operations
c) Reports will be handled confidentially, and appropriate action will be taken to safeguard the integrity of the organisation's systems and records.

10. TESA IT Equipment

a) ETT provides pool laptops and PCs for Learners to use whilst at TESA.
b) It is the Learner of User's responsibility to log out of any systems or platforms and shut down the machine fully.
c) All IT Equipment is fitted with Freeze software – this removes the previous user's data from the machine when switched off and re-booted.
d) It is the Learner's responsibility to shut down the machine fully to allow the Freeze to operate correctly.

11. Internet Use – TESA Wi-Fi

a) The Internet is a valuable resource and necessary for you to successfully undertake your role or learning.

b) Reasonable private use of TESA Wi-Fi is permitted during break and lunch times but should be kept to a minimum. Private use is not acceptable during working hours (User) or during timetabled sessions (Learners).
c) Internet connection for Learners is filtered to prevent access to inappropriate sites and content.

12. Bring Your Own Device (BYOD) and Off Site Access

a) Learners and employers may use Personal Devices to access ETT IT Platforms (such as OneFile, ARP, or email) provided they comply with the following security requirements:
    i. Multi Factor Authentication (MFA) must be enabled on any personal device used to access ETT platforms.
    ii. Personal devices must have up to date antivirus software and, where ETT data is stored locally, the device storage must be encrypted.
    iii. ETT accepts no responsibility for data costs, loss of personal data, or damage to personal devices arising from accessing ETT systems.
    iv. You must log out of all ETT platforms when you finish using them, especially on shared or family devices.
    v. You must not leave ETT data visible on a personal device in an unsecured public place.
    vi. Failure to follow these requirements may result in suspension of remote access pending a review.

13. Reporting a Security Incident

a) A security incident is any event that compromises the confidentiality, integrity, or availability of ETT information or IT systems. All Learners have a duty to report suspected incidents immediately.
b) Reporting Procedure:
    i. All incidents must be reported within one hour of discovery to both:
        1. The Chief Executive, and
        2. The Director of Delivery and Operations
c) Provide all known details: what happened, when, and what device or data was involved.
d) Do not attempt to investigate or fix the problem yourself, unless instructed by the Chief Executive or IT Support.
e) The Chief Executive will then activate the incident response process, which will involve our external IT support provider and, if necessary, external reporting (e.g. to the ICO).

14. Personal Email

a) Learners may access personal email accounts whilst on IT Equipment and/or ETT networks.
b) Learners must protect the IT Equipment and/or ETT network from viruses and/or other malicious software.
c) Users and Learners must check all incoming attachments or links before clicking on them to open.
d) Check the email address has a genuine URL that is related to the sender or sender's organisation.
e) Ensure any attachment is a genuine document files (.DOC, .XLS, etc.) and are not executable files (.COM, .EXE, etc.) which may carry viruses.

f) Ensure installed virus protection within the email provider's platform is up to date and valid.
g) If in doubt, do not click or open any attachments.
h) Any incidents that may introduce viruses and/or other malicious software onto a piece of IT Equipment, IT Platform or ETT Network should be reported immediately using the process set out in 12.b.

15. Sharing Responsibilities

a) Where there is a requirement to share information with others using a cloud storage service, then it is important that individuals who enable the sharing of data do so with the following safeguards:
b) Grant access only to the specific folders and files that are required to support the collaboration or information sharing.
c) Ensure that no other folders or files are made available.
d) Take care to ensure access is granted to the correct individuals.
e) Inform all individuals involved in the collaboration or information sharing that they have a duty of care for the information provided and must honour all security requirements as well as privacy and confidentiality commitments.

16. Social Media

a) Freedom of speech and academic freedom are central to ETT's approach to learning, including in a social media context, and nothing in this guidance is intended to compromise these fundamental freedoms.

17. Social Media Etiquette

a) We expect Learners and Employers to use social media in a positive way, and we are happy to be mentioned or tagged in any such posts.
b) When using social media, it can be tempting to speak and act in a way we would not face to face. Remember that innocently intended comments posted online are more easily misconstrued, as online writing can lack the nuances of face to face interaction.
c) Consider when posting online:
    i. Who is the audience for your post?
    ii. Will it be limited to close friends and family or could it be read by the wider public?
    iii. Could it be seen by people you have, or might one day have, a professional relationship with?
    iv. Remember that in most cases, content you post will be public, it may not be possible to remove it at a later date, and it could be reposted or shared through other forms of social media.
    v. Think twice about how you post content if you are feeling angry about something and consider the effect that this might have on the situation.
    vi. If you are responding to someone else's post, ask yourself whether you are sure that you have read the post in the way in which it was intended. Your response could just escalate a situation.
    vii. Using social media to post offensive or abusive comments, images or other content may constitute a breach of the ETT code of conduct and could result in disciplinary action.
    viii. This can be via your association to ETT even if the post has no mention of us or relevance to us.
    ix. This could include (but not limited to):

1. serious misconduct including harassment or bullying
2. accessing, downloading, or storing inappropriate material
3. bringing the ETT name into disrepute
4. bringing your employer's name into disrepute

18. Cyberbullying and off platform behaviour

a) Cyberbullying includes sending threatening or abusive messages, excluding others deliberately, sharing embarrassing images without consent, or creating fake profiles to harm someone. This policy applies to behaviour on any social media platform or messaging service, even outside college hours and off ETT premises, where that behaviour affects a learner's ability to participate in their programme or damages the reputation of ETT.

b) Learners who experience or witness cyberbullying by another learner (for example in a WhatsApp group or on Discord) must report it to a staff member or the DSL. Screenshots may be requested as evidence. ETT will take disciplinary action against learners found to have engaged in cyberbullying, which may include suspension or withdrawal from the programme.

c) Using social media to complain about ETT services or actions.

d) If Learners or Employers have a complaint or grievance about our services or actions, we ask them to raise it with an ETT staff member so it can be resolved.

e) We have both informal and formal complaint procedures that can address any issues – please see the Complaint and Grievance Policy and Procedure.

19. Social media boundaries between staff and learners

a) To maintain professional boundaries and safeguard young people, ETT staff and assessors must not:

i. accept friend or follow requests from learners on personal social media accounts,

ii. send private messages to learners via personal social media accounts, or

iii. use WhatsApp, Snapchat, Discord, or any similar platform for one to one communication with a learner unless an approved group for cohort announcements exists and all messages are visible to a manager.

iv. If a learner sends a friend request to a staff member on a personal account, the staff member must decline it and report the interaction to the DSL. Professional communication must take place only through ETT approved channels: email, OneFile, the Apprentice Review Portal, or the official ETT Microsoft Teams environment.

v. Learners are expected to respect these boundaries and not to seek out staff members on personal social media platforms.

20. Safeguarding and Prevent

a) Any online interaction, whether on ETT systems or personal social media, that suggests a learner may be at risk of harm, exploitation, radicalisation, or involvement in extremist activity must be reported immediately to the Designated Safeguarding Lead (DSL) or any member of staff, who will then follow the procedures set out in the separate Safeguarding and Prevent policies. This includes receiving messages from strangers, being asked for private information, or being shown violent or extreme content. Do not delete the messages before reporting them.