INFORMATION TECHNOLOGY POLICY & PROCEDURE

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 in the pursuit of the work undertaken by Engineering Trust Training (ETT). 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 staff at partner businesses or subcontractors.
3. **Definitions**
    a) User -- ETT member of staff who is given access to an ETT Microsoft account and other ETT equipment and platforms.
    b) Learner -- An ETT Apprentice or learner who has access to OneFile and/or attends The Engineering Skills Academy (TESA).
    c) 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.
    d) IT Equipment -- Electronic devices owned and controlled by ETT.
    e) 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.
    f) Personal Device -- An electronic device not owned by ETT.
    g) ETT Network -- The infrastructure provided by ETT at TESA including internet connection, cabling and servers.
4. **Roles and Responsibilities**
    a) ETT Users, 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 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.
    c) 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. This includes, but is not limited to:

i. Implementing and managing firewalls, internet content filtering, and antivirus/anti- malware solutions
ii. Ensuring the regular, tested, and secure backup of all critical ETT data
iii. Applying security patches and updates to all IT Equipment and servers in a timely manner
iv. Configuring and enforcing Multi-Factor Authentication (MFA) on all applicable accounts and platforms
v. Monitoring systems for security breaches and responding to technical incidents as part of a formal agreement

5. Unacceptable Use

a) IT Equipment, IT Platforms and the ETT Network may not be used directly or indirectly by a User or Learner 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.
b) Uploading ETT data into public AI tools is prohibited unless approved in accordance with the Section 6 - External Platforms & Data Handling
c) IT Equipment, IT Platforms and the ETT Network may not be used directly or indirectly by a User or Learner for activities having, or likely to have, any of the following characteristics:
   i. Intentionally wasting staff effort or other ETT resources
   ii. Corrupting, altering or destroying another User or Learner's data without their consent
   iii. Disrupting the work of other Users or Learner
   iv. Denying access to other users or Learners
   v. Pursuance of commercial activities outside of those in support of ETT business or learning activities.

d) 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.
e) Users and 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) Core Principle
    i. 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:
    i. Public or consumer-grade Artificial Intelligence tools (e.g. ChatGPT, Google Bard, Microsoft Copilot – consumer version)
    ii. Consumer cloud services (e.g. SurveyMonkey, MailChimp, JotForm, Canva)
    iii. Free or personal-tier applications
    iv. Any platform not covered by an ETT business contract or data-processing agreement
c) Rationale
    i. This requirement protects ETT from data breaches, loss of control, non-compliance with GDPR, and exposure to insecure or unregulated services.
d) Permission Process
    i. Users must obtain explicit written approval from the Chief Executive before uploading any ETT data into an external service.

7. PINs, Passwords, MFA, and Electronic Signatures

a) Principles
    i. Always keep passwords and PINs safe and secure
    ii. Do not allow another User, 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 Users, 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 User, 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 User, 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 a User, 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. Users, 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) Multi-Factor Authentication (MFA)
   i. MFA (also known as Two-Factor Authentication or 2FA) is a mandatory security control to protect ETT data and systems.
   ii. All Users must enrol and use MFA on their ETT Microsoft account (Office 365) and any other ETT-approved platform that supports it (e.g. Claris, OneFile).
   iii. MFA requires something you know (your password) and something you have (e.g. a code from an authenticator app on your phone, or a hardware token). This provides significantly stronger protection than a password alone.
   iv. Users must not disable, bypass, or share their MFA method. Any attempt to do so will be treated as a serious security breach.

d) 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. Users, 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. Users, 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 User, Learner or Employer knowingly uses another person's Password it reduces the security and integrity of that equipment, platform or network.

e) Electronic Signatures: An electronic method of indicating agreement or approval of a document.
   i. Users, 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 a User, Learner or Employer, must be reported this 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 switch off and re-booted.
d) It is the Learner of User's responsibility to shut down the machine fully to allow the Freeze to operate correctly.

11. Internet Use – TESA Wifi

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

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

12. ETT Email use

a) Learners are not issued an ETT controlled email address.
b) Users will be issued with a ETT controlled (work) email account specific to them. It is therefore each user's responsibility to use the account in an appropriate manner.
c) Users should be clear that the data and communication held on or sent/received via a work email account is the property of ETT and not that of the User. It is advised that Users do not conduct personal matters via their work email account.
d) Specific areas Users must consider when using a work email account include;
    i. Security of Information - preventing information from falling into the wrong hands.
    ii. Appropriate Use - using email facilities for the purposes for which they are provided.
    iii. Legal Issues - not using email for purposes which are illegal, or which breach confidentiality or privacy.
    iv. Retention and Compliance - some email may be required as part of an investigation or legal proceedings.
e) Email accounts are provided for communication purposes and messages should be accurate, courteous and necessary. Messages should not be sent to a larger audience than is reasonably justifiable, particularly when they contain attachments.
f) Email accounts must not be used to defame others.
g) Users must not leave IT Equipment logged into their email account unattended, unless it is disabled by a password protected screen saver.
h) Users must not leave their password written on a piece of paper adjacent to IT Equipment. Other people may use it to gain access to the User's e-mail and may impersonate them sending an email. The Chief Executive will hold a record of a User's password to ETT controlled systems for business continuity reasons.
i) Users must not disclose passwords to others.
j) If Users receive email purporting to come from a particular individual, but out of character with their normal style, treat it as the result of possible impersonation until confirmation or legitimacy is gained.
k) Users must take great care when addressing e-mail messages, to avoid incorrect delivery, this is particularly true when sending email addresses which consist primarily of numbers. Users are most at risk when sending email to people with whom they have never communicated before, or infrequent correspondents for whom they do not have an alias set up. If sending important information, it is

often helpful to have the intended recipient email first and use the email 'Reply' facility which will ensure that the correct address is used.

l) Users are well advised not to send, via e-mail, material which they would not be happy sending in an unsealed envelope, unless they have made explicit arrangements to exchange the material via a secure e-mail channel with the recipient.

m) Users must check all incoming attachments or links before clicking on them to open.
    i. Check the email address has a genuine URL that is related to the sender or sender's organisation.
    ii. Ensure any attachment is a genuine document files (.DOC,.XLS, etc.) and are not executable files (.COM, .EXE, etc.) which may carry viruses.
    iii. Ensure installed virus protection (Windows Security) is kept up to date.

n) Bear in mind that legal proceedings may result from inadvertent or negligent disclosure of confidential information.

o) E-mail may be treated as written evidence in law. Any email which forms part of a commercial negotiation or contract for goods, services or employment might be required as evidence in a court of law. These emails should never be deleted and kept for future reference.

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 Users and Learners have a duty to report suspected incidents immediately.

b) Examples of security incidents include:
    i. Suspected phishing emails (especially if a link was clicked or an attachment opened)
    ii. Loss or theft of IT Equipment (laptop, phone) or any device used for work
    iii. Seeing someone access data or a system they should not have
    iv. Realising you have disclosed your password or PIN to someone else
    v. Ransomware or other malware infection (e.g. files won't open, strange messages appear)
    vi. Accidental sharing of data with the wrong person

c) Immediate Steps:
    i. For a suspected technical breach (e.g. phishing click, malware): Immediately disconnect the device from the internet and the ETT Network (turn off Wi-Fi and unplug network cables). Do not turn the device off.
    ii. For a lost or stolen device: Immediately report this to the Chief Executive and, if applicable, the police.

d) 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

ii. Provide all known details: what happened, when, and what device or data was involved.
iii. Do not attempt to investigate or fix the problem yourself, unless instructed by the Chief Executive or IT Support.
iv. 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) Users and Learners may access personal email accounts whilst on IT Equipment and/or ETT networks.
b) Users and 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.
    i. Check the email address has a genuine URL that is related to the sender or sender's organisation.
    ii. Ensure any attachment is a genuine document files (.DOC, .XLS, etc.) and are not executable files (.COM, .EXE, etc.) which may carry viruses.
    iii. Ensure installed virus protection within the email provider's platform is up to date and valid.
    iv. If in doubt, do not click or open any attachments.

15. Access

a) ETT reserves the right, without notice, to access, listen to or read any communication made or received by a User on IT Equipment including computer, mobile phone or telephone for the following purposes:
    i. to establish the existence of facts, to ascertain compliance with regulatory or self-regulatory practices and procedures
    ii. for quality control and employee training purposes
    iii. to prevent or detect crime (including 'hacking')
    iv. to intercept for operational purposes, such as protecting against viruses and making routine interceptions such as forwarding emails to correct destinations, and
    v. to check voicemail systems when the employee is on holiday or on sick leave.

16. Remote and Mobile Working

a) Many Users work remotely, at employer premises, or from home. The security of ETT data must be maintained regardless of location.
b) When working away from TESA, Users must:
    i. only connect to secure, password-protected Wi-Fi networks. Do not conduct ETT business using public, open, or untrusted networks (e.g. in coffee shops, hotels, airports).

ii. Ensure that laptop screens and mobile devices cannot be viewed by unauthorised people (e.g. on trains, in public spaces). Use a privacy screen if necessary.
iii. Never leave IT Equipment unattended in a vehicle, hotel room, or any other public place. When not in use, devices must be stored securely.
iv. Be aware of your surroundings when taking work calls or discussing learner information to avoid unintentional disclosure.

c) All portable IT Equipment (laptops, tablets, phones) used to access ETT data must have full-disk encryption enabled and be password/PIN protected.

17. Cloud Services & Storage

a) Cloud Services and Storage are used in relation to the work done by ETT and applies to all Users, Learners and other parties who have access to those services and/or ETT data held on those services.

b) Cloud Services & Cloud Storage relate to the storage and/or processing of ETT data therefore this policy should be read in conjunction with the Data Retention, Data Protection and Privacy
policy for more information about how/why data is collected and how long the data will be held.

c) Cloud Services are defined as services provided by an external supplier and made available to organisations, or individuals under terms and conditions which are defined by the external
supplier.

d) Cloud Services are provided on infrastructure external to the ETT Network and include platforms used to operate ETT such as Claris, OneFile, BKSB, JotForm etc.

e) Cloud Storage is used to facilitate the sharing of files and make data available over a range of computers and other mobile devices, usually accessed via options including: web browser; mobile app; synchronisation client; drive mapping. Cloud storage controlled by ETT is on Microsoft OneDrive and Users are required to use this when sharing ETT data. Learners may use other platforms to share information with ETT, examples include: Dropbox, Box, Microsoft OneDrive, Apple iCloud, Google docs.

f) Business services are those that ETT enter into a contract with and are specifically designed for business use. Organisations (ETT) contract with their preferred provider for specific services and manage the accounts for the individuals within their organisation who they wish to have access.

g) Business orientated cloud services and storage should be used where possible as they mitigate much of the risk when using a consumer service, in particular:
i. The terms and conditions and service level agreement is tailored to business needs.
ii. The organisation retains full ownership of their data.
iii. Security of data is sometimes assured via industry standard accreditations e.g. ISO 27001.

iv. Data retention and backup arrangements are defined.
v. There is no advertising built from data mining or other uses of data.
vi. The provider's liability relating to negligence, misuse, loss or damage of data is better defined.
vii. As they mitigate significant risk, business-oriented services should be used as much as possible.
viii. Consumer services are those where the contract is with an individual and often made available free of charge to individuals via a user registration process or bundled initial hardware purchases. When signing up to provider of this type, the individual must accept the provider's Terms and Conditions and any associated service level agreement. Consumer cloud services can offer many benefits to ETT and may be used however; the risks must be taken into consideration and the amount of data uploaded to the platform should be limited to the minimum required. Risks include:
    1. no guarantee on data protection, retention or backup and
    2. platform may store data outside the UK/EU and not be bound by UK/EU laws relating to the protection of personal data.
ix. Individuals should read carefully the Terms and Conditions governing the use of the platform with reference to;
    1. circumstances leading to account termination and potential loss of data
    2. provider's liability for negligence with respect to misuse, exposure, loss or damage of data
    3. confidentiality of data with respect to provider's data mining activities and potential resale of information for advertising, user tracking and user profiling purposes.
    4. considerations about who owns the data and therefore has full rights over it. Some cloud providers may assert ownership of any data stored in the provider's cloud or reserve the right to do so in future.
    5. the financial stability of cloud providers should be considered to avoid a potential end of service with no or little notice, and
    6. the risk reduction measures on both business and consumer services.

h) Users must:
    i. ensure they understand the requirements relating to the storage and guardianship of ETT data (see relevant policies)
    ii. safeguard the security, confidentiality, integrity and availability of ETT information assets and data
    iii. ensure compliance with national and international laws governing the storage and guardianship of data, and

iv. ensure compliance with contractual commitments relating to the storage and guardianship of data.

18. Business Services

a) Users may only store or process data using the ETT cloud service, hosted on Microsoft Office365 e.g. OneDrive, SharePoint.

b) Applicant data will be held on the Claris (ETT LMS) platform. Additionally, data will be held on the Selecta-head system.

c) Employer and Learner data will be held on Claris (ETT LMS) platform and the e-portfolio platform OneFile.

19. Consumer Services

a) Use of consumer cloud services for storing or processing ETT data is only permitted where approved under Section 6 - External Platforms & Data Handling requirements of this policy.

20. Backups

a) Critical ETT data held in cloud services (e.g. OneDrive, SharePoint, Claris, OneFile) is backed up by the respective service providers. Users do not need to create personal backups.

b) However, Users are responsible for saving all work-related files to the approved ETT cloud storage (OneDrive/SharePoint) and not solely to their local device hard drive. Data stored only on a local laptop is at risk of irretrievable loss if the device is lost, stolen, or damaged.

21. 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:

i. Grant access only to the specific folders and files that are required to support the collaboration or information sharing.

ii. Ensure that no other folders or files are made available.

iii. Take care to ensure access is granted to the correct individuals.

iv. 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.