

# INFORMATION TECHNOLOGY POLICY & PROCEDURE

## 1) Purpose

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. 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.
- b) Learner – An ETT Apprentice or learner who has access to OneFile and/or attends The Engineering Skills Academy (TESA).
- c) IT Equipment – Electronic devices owned and controlled by ETT
- d) Personal Device – An electronic device not owned by ETT.
- e) ETT Network – The infrastructure provided by ETT at TESA including internet connection, cabling and servers.

## 4) Unacceptable Use

- a) IT Equipment and/or 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;
  - ix) material that brings ETT into disrepute.
- b) IT Equipment 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.
- 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.
- d) Users and Learners shall not:
- i) introduce data-interception, password-detecting or similar software or devices to the ETT IT equipment or 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;
  - vi) add ETT data to an un-authorised cloud service without the permission of the Chief Executive.

#### **5) Password Guidance**

- a) Always keep passwords safe and secure.
- b) Do not allow any other User or Learner to use a machine that is logged in under your name.
- c) Do not use any ID which is not your own or use a piece of IT Equipment which is logged on under an ID which is not yours, unless authorised to do so by the Chief Executive.
- d) Create a password that is not a name or a complete word, nor a common abbreviation. A combination of eight letters/numbers or more is recommended.
- e) You must take care not to leave IT Equipment logged on under your user ID, which would allow other Users or Learners to access the network in your name.
- f) Change your password regularly (you will periodically be prompted to do so by some systems). Avoid writing down your password.

#### **6) Internet Use**

- a) The Internet is a valuable resource and necessary for you to successfully undertake your role or learning
- b) Reasonable private use of the internet 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) Be aware that Internet use at TESA is often monitored and may include a record of sites visited using both IT Equipment and Personal Devices.

#### **7) 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;

- 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.

## 8) 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.

#### **9) Access**

- a) ETT reserves the right, without notice, to access, listen to or read any communication made or received by a User on their 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.

#### **10) 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 is 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.

- i) 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:
  - (1) The terms and conditions and service level agreement is tailored to business needs.
  - (2) The organisation retains full ownership of their data.
  - (3) Security of data is sometimes assured via industry standard accreditations e.g. ISO 27001.
  - (4) Data retention and backup arrangements are defined.
  - (5) There is no advertising built from data mining or other uses of data.
  - (6) The provider's liability relating to negligence, misuse, loss or damage of data is better defined.
  - (7) As they mitigate significant risk, business-oriented services should be used as much as possible.
- g) 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:
  - i) There is no guarantee on data protection, retention or backup
  - ii) The platform may store data outside the UK/EU and not be bound by UK/EU laws relating to the protection of personal data.
  - iii) 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.
- h) Risk reduction measures on both business and consumer services. 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;
  - iv) ensure compliance with contractual commitments relating to the storage and guardianship of data.

- i) Business Services
    - i) Users may only store or process data using the ETT cloud service, hosted on Microsoft Office365 e.g. OneDrive, SharePoint
    - ii) Applicant data will be held on the Claris (ETT LMS) platform. Additionally, data will be held on the Selecta-head system.
    - iii) Employer and Learner data will be held on Claris (ETT LMS) platform and the e-portfolio platform OneFile.
  - j) Consumer Services
    - i) Users must seek permission from the ETT Chief Executive before uploading any ETT data into such services. Service examples
      - (1) Survey Monkey
      - (2) Mail Chimp
      - (3) JotForm
      - (4) Canva
  - k) Sharing Responsibilities
- 11) 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. Ensure that no other folders or files are made available.
  - ii) Take care to ensure access is granted to the *correct* individuals.
  - iii) 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.