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 so as 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) IT Equipment – Electronic devices owned and controlled by ETT
c) ETT Network – The infrastructure provided by ETT at its Head Office including internet connection, cabling, servers and other electronic devices.

4) Unacceptable Use

a) IT Equipment and the ETT Network may not be used directly or indirectly by a User 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 on the basis of 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 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's data without their consent.
   iii) Disrupting the work of other Users.
   iv) Denying access to other users.
   v) Pursuance of commercial activities outside of those in support of ETT business.
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 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) Keep passwords safe and secure at all times.
b) Do not allow any other user 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 machine 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 computers/mobile devices logged on under your user ID, which would allow other users 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.
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 day.
c) Be aware that Internet use is often monitored and may include a record of sites visited.

7) E-mail use

a) Users will be issued with a work email account specific to them. It is therefore each user's responsibility to use the account in an appropriate manner.
b) 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.
c) 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 e-mail facilities for the purposes for which they are provided.
iii) Legal Issues - not using e-mail for purposes which are illegal, or which breach confidentiality or privacy.
iv) Retention and Compliance - some e-mail may be required as part of an investigation or legal proceedings.
d) E-mail 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.
e) Do not leave a machine which is logged into your e-mail account unattended, unless it is disabled by a password protected screen saver
f) Do not leave your password written on a piece of paper adjacent to your machine. Others may use it to gain access to your e-mail and may impersonate you in sending e-mail. Whilst the Chief Executive may hold a record of your password for business continuity reasons, you should not disclose it to others.
g) If you receive e-mail purporting to come from a particular individual, but out of character with their normal style, treat it as the result of possible impersonation until you have had the chance to confirm it as genuine.
h) Take great care when addressing e-mail messages, to avoid incorrect delivery, this is particularly true when sending e-mail addresses which consist primarily of numbers (such as

learner addresses). You are most at risk when sending e-mail to people with whom you have never communicated before, or infrequent correspondents for whom you do not have an alias set up. If sending important information, it is often helpful to have the intended recipient e-mail you first and use the e-mail 'Reply' facility which will ensure that you get the address correct.

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

j) Check all incoming attachments before clicking on them to open. Ensure that they are genuine document files (.DOC, .XLS, etc.) and are not executable files (.COM, .EXE, etc.) which may carry viruses. Install a reliable virus protection program and ensure that it is kept up-to-date.

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

l) E-mail may be treated as written evidence in law. Any e-mail 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.

m) Ensure that e-mail is not used to defame others.

8) Access

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

9) Cloud Services

a) Cloud services are defined as services provided by an external supplier and made available to organisations, or individuals, on terms and conditions, which are defined by the external supplier. Cloud services are provided by infrastructure external to the organisation's domain (data centres). Cloud storage services 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 provider examples include: Dropbox, Box, Microsoft OneDrive, Apple iCloud, Google docs. They also refer to platforms used to operate the organisation such as Enrola, Smart Assessor, Jotform.

b) Cloud services relate to storage 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 we collect this data and how long the data will be held.

c) The policy applies to all ETT data i.e. information which arises from the work done and applies to all staff, learners and other parties who have access to ETT data.

d) Services highlighted below may be used. Below also identifies the measures required to reduce the risks to acceptable levels. This is in order to:

   i) ensure that ETT employees and other partners understand the requirements relating to the storage and guardianship of data;

   ii) safeguard the security, confidentiality, integrity and availability of ETT information assets;

   iii) snsure 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.

e) Services
   i) HQ Data may only be stored or processed using the ETT cloud service, hosted on Microsoft Office365.
   ii) Applicant data will be held on the Enrola platform and e-Store which is being de-commissioned. Additionally, data will be held on the Selecta-head system.
   iii) Employer and learner data will be held on the Smart Assessor platform
   iv) Other data will also be held on ad-hoc platforms such as Survey Monkey, Mail Chimp, Jotform and other online tools.

f) Business services - where the contract is with an organisation/company.
   Some cloud service providers offer services specifically designed for business use. Organisations contract with their preferred cloud service provider for specific services and manage the accounts for the individuals within their organisation who they wish to have access. Business orientated cloud services 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.

g) Consumer services - where the contract is with an individual.
   Consumer-orientated cloud services are often made available free of charge to individuals via a user registration process, or bundled initial hardware purchases. When signing up with a cloud service provider, the individual must accept the provider's Terms and Conditions and any associated service level agreement. Consumer cloud services can offer many benefits to the business 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 particular reference to;
      - Circumstances leading to account termination and potential loss of data
      - Provider's liability for negligence with respect to misuse, exposure, loss or damage of data
      - Confidentiality of data with respect to provider's data mining activities and potential resale of information for advertising, user tracking and user profiling purposes.
      - Considerations about who actually 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.
      - The financial stability of cloud providers should be considered to avoid a potential end of service with no or little notice.

h) Sharing Responsibilities

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.