e-Safety Policy & Agreement for Staff Members

e-Safety Policy Statement

ITEC is in place to 'Accelerate workforce development for tomorrows challenges', we our core values are;

- **Getting learners future-fit through quality provision and pace**
- **Utilising technology in the way we work and deliver**
- **Creating career pathways**
- **Focus on businesses where we can add value**
- **Training diverse people and being inclusive**
- **Adding value through insight and research**

It is therefore important to ensure we are able to deliver a quality service, ensuring learners are future-fit, whilst maintaining the importance of both utilising and leading in the way we use technology.

This policy and agreement has been drawn up to protect learners, ITEC staff and members of the public. All staff members will be asked to sign a copy of the agreement and return it to the Managing Director prior to using the ITEC's facilities. Staff members may use ITEC's computer systems to enhance their professional activities including training, research, assessment, communication, administration and management.

1. General e-Safety Policy

Staff members will only use ITEC-provided items for storage of any media with regards to ITEC learners, apprentices, employers and staff including photographs, blogs, assessments materials, etc. Photographs can only be taken of learners, apprentices, staff and employers with their permission and for the use of posterity or marketing activities. Photographs must not be taken using the staff member's personal camera or mobile phone, photographs must have the consent of the person/s being photographed. Any photos that are taken must be transferred for storage to the appropriate folder on the ITEC's Exchange directory and local copies on the device deleted.

Communication between staff members and learners, by whatever method, should take place within clear and explicit boundaries. Staff members should not share any personal information with a young person or vulnerable adult nor should they request or respond to any personal information from them, other than that which might be appropriate as part of their professional role.

All communications should be transparent and open to scrutiny, all comms with learners must be via an ITEC platform or device. Staff members need to be mindful that with technology the potential for messages to be seen out of context or mis-interpreted is increased. They should not share their personal e-mail addresses and mobile phone numbers with learners, unless approved by a line manager. In all cases, ensure that their relationships with young people are known and approved by senior staff.

Storage of learners' personal information, including reports and appraisals, must be secure at all times. Memory sticks and disks are not secure and must be protected from loss or theft. Personal and confidential information will be stored on ITEC's network in a secure area and removed from the laptop or desktop PC. Laptops and desktop PCs must be locked when not in use, or when stepping away from your desk for a short time, especially if they are in an area where the information can be seen by learners and/or other members of staff. All Learner data must be stored on an ITEC approved device/solution and must never be transferred to a non ITEC approved storage medium.

2. **Social Networking and Media Sites**

Staff members using social networking and media sites must take responsibility for security settings and strong passwords should be applied to ensure control of access to personal profiles, 2 Factor should be enabled on all sites that support this option. Staff members should ensure they set profiles to private, and remove from searches, and ensure security settings are checked.

Staff members will not under any circumstances search or look up learners, and must not add or follow active learners or apprentices to their personal social networking pages. If a site suggests following or adding a friend that is a Learner, then you must block and reject the suggestion.

If a learner attempts to make contact, connect, follow or friend you on a social networking or media site, this should be reported to the Safeguarding team immediately.

Staff members should ensure that images, posts and items shared on social media, blogs, message boards, and websites are appropriate and representative of ITECs policies, ideals and brand.

The minimum age of use of any social networking site must be observed by ITEC staff at all times. If social networking or instant messaging sites are to be used as part of courses being delivered by the ITEC, a separate and approved account must be set up for this purpose and agreed with senior management. All users of the system must be authenticated.

3. Laptop Policy

ITEC may assign laptop computers to members of staff to be used solely for the purpose of conducting ITEC business and carrying out their work duties. This laptop remains the property of ITEC and ITEC reserves the right to recall the laptop for use, withdrawal or inspection at any time. ITEC also reserves the right to remote access devices and storage at any time.

Staff members must be vigilant about what is stored on their laptop when they are using it at home. Laptops are provided for work use, and should not be used by anyone other than the person they are assigned to. Friends and family members are not to use work devices for security and safeguarding reasons.

The staff member is responsible for all materials stored on their allocated laptop and will be culpable in situations where e-safety or e-security is compromised and/or inappropriate materials are found to be present. Although the laptops are insured against loss, staff members are expected to take reasonable steps to ensure the safety and security of the laptop at all times.

3.1. The laptop must not be left unattended on visits to employers' premises
3.2. The laptop must not be left unattended in a vehicle or, where this is unavoidable, it must be locked in the boot out of sight.

3.3. The laptop must not be connected to any other network other than ILT without authorisation
3.4. Any damage or malfunction must be reported to technical support or the Technical Trainer
3.5. Any software installed on the laptop must be authorised prior to installation
3.6. Used of third party hardware must be authorised to ensure compatibility with ITEC systems

4. Remote Working Policy

When working remotely, either from home, another campus, or when visiting a client, laptops must be kept secure. Staff members must ensure information being displayed is appropriate to anyone who may be in view. At no point must private or student data be visible to another person outside of ITEC.

Staff must ensure they are using the laptop for business purposes only, ITEC laptops are not for personal use, and should only be used by the person assigned to that device.

If a member of staff has access to remote working or VPN, they must ensure they are using this during work hours, or agreed hours only. Access outside of work hours without express permission is prohibited.

5. Internet Policy

Where internet research is required as part of a course, the trainers must test key word searches and sites prior to the learning session to check for any inappropriate sites that may come up innocently in the search. Learners must not 'publish' work on-line as part of the course unless specifically authorised by the trainer within an allocated safe site.

Authorisation should be sought prior to any software being downloaded from the internet. Staff members will be responsible for all e-mails sent and received on their accounts and must be vigilant about the risk of virus infection from files attached to e-mails.

All internet activity will be appropriate to the staff member's professional use. Staff members must not use the internet for personal financial gain, gambling, political purposes, advertising or any other use deemed as not conducive to business practice.

Copyright of materials must be respected at all times. The use of chat rooms is strictly forbidden and the use of ITEC's network to knowingly access inappropriate materials such as pornographic, racist or offensive material is strictly forbidden and may constitute a criminal offence.

6. E-mail Policy

ITEC's e-mail system must not be used for sending private or personal messages and anonymous messages and/or chain letters must not be forwarded. The same professional and business standards of communications applied to letters and other media will also apply to the content of e-mails, including the language used.

Staff should not send unsecure emails for private and confidential data or information, and should ensure information is sent securely when required.

7. BYOD/Mobile Policy

Staff should follow all ITEC policies when using a personal device or mobile at ITEC.

Last Reviewed	23 February 2021
Reviewed by	Ben Turner

Staff should be aware of applications and websites used whilst connected to the ITEC systems, and ensure they follow ITEC policies.

When connected to ITEC systems and Wi-Fi, staff will ensure IT policy is followed, and they are not looking up content that would otherwise be inappropriate if using an ITEC issued device.

Any loss of a device with ITEC access used for BYOD must be reported immediately. This includes personal mobile devices with access to ITEC email.

8. Monitoring Policy

ITEC reserve the right to monitor all activity on the ITEC network, Internet and email usage. All Internet activity is logged and monitored to ensure safeguarding and the IT policy is followed.

ITEC will monitor emails coming in and being sent from the business.

ITEC reserve the right to check and ensure social networking and media follow the IT standards and representation of the business.

Staff members are reminded it is illegal to:

- View, possess or distribute indecent images of a person under 18
- Incite hatred on the basis of race, religion, sexual orientation, gender, etc.
- Harass or threaten any individual, including cyber-bullying by mobile phone, social networking sites, etc.
- Send indecent, offensive or threatening messages with the purpose of causing the recipient distress or anxiety

Staff members are reminded it is inappropriate to:

- Post offensive or insulting comments about the ITEC, any staff member, any employer or any learner/apprentice on social networking sites
- Access adult pornography, sites of a sexual nature (including shopping sites for fetish equipment or sexual aids) and gambling sites on ITEC computers at all times, including breaks
- Make derogatory comments about learners, employers or colleagues in e-mails, in texts and on social networking sites
- Contact learners on social networking sites and media sites
- Contact learners personal e-mail addresses unless for legitimate purposes related to the course or apprenticeship

9. Reporting Policy

All staff should be aware that it is everyone's responsibility to ensure security and safeguarding is followed.

Staff should report all security concerns, spam/scam emails, and IT issues to the IT team to resolve.

Staff should report any damage, lost or stolen devices, or potential data breaches to the IT team immediately they are discovered.

Last Reviewed	23 February 2021
Reviewed by	Ben Turner

All staff should be vigilant for breaches of safeguarding, and report any behaviour or concerns to the safeguarding team.

10. E-safety, Laptop and Internet Agreement

I have read and understood the above conditions and agree to abide by them.

11. Training and Support

ITEC are here to support our staff members to ensure proper understanding of this policy but also to offer advice on how to implement accordingly. ITEC will brief staff on a yearly basis (and new staff on joining) about the IT policy and look to offer guidance where applicable.

Name:	**Laptop Assigned (Serial No):**
Signed:	**Date:**

Last Reviewed	23 February 2021
Reviewed by	Ben Turner