10th Anniversary
Training Apprentices since 2011

ELA TRAINING SERVICES

E-Safety Policy

Suite 104, 1 Meadlake Place, Thorpe Lea Road, Egham, Surrey, TW20 8HE | +44 208 017 1425 | info@ela-training.co.uk

Key Elements

This document sets out the responsibilities and expectations for all employees of The ELA Training Services in relation to and promoting the health, safety, wellbeing, ethical and professional conduct and safeguarding of all stakeholders of the ELA Training Services.

Implementation is monitored by the Managing Director and supported by the board of Directors.

Agreed by Inderjot Singh, Managing Director,
ELA Training Services.

ELA TRAINING SERVICES' E-Safety Policy

Purpose

This policy applies to all members of the ELA Training Services community (including staff, children, employers/carers and visitors). It is a statement of the aims, principles, strategies and procedures for e-safety throughout ELA Training Services. The E-Safety Policy should be read in conjunction with our Data Protection and Information Sharing Policy and Safeguarding Policy.

We have a responsibility to the learners in our care to know what they are doing online during their stay with us.

What is E-Safety?

E-Safety refers to safeguarding and safeguarding of both children and adults in the digital world. It is about learning to understand and use technologies in a safe, positive way, also about supporting children and adults to develop safe online behaviours.
Risks to children who use the internet include:

- Exposure to inappropriate materials, for example, pornographic pictures and videos
- Physical danger and sexual abuse, for example, through 'grooming' by paedophiles
- Cyber bullying-persistent bullying through the digital medium

- Physical danger and sexual abuse, for example, through 'grooming' by paedophiles
- Cyber bullying-persistent bullying through the digital medium
- Losing control over pictures and videos
- Obsessive use of the internet and ICT, for example, addiction to video games
- Damage to online reputation
- Inappropriate or illegal behaviour, for example, exposure to hate mail or offensive images

  viruses, hacking and security
- Exposure to extremist material and the possibility of radicalisation
- Copyright infringement, for example, the illegal sharing of music, pictures, video or documents

E-Safety is largely concerned with internet communications. The internet is accessible from computers, laptops, tablets, mobile phones, games consoles and other devices like the iPod Touch and internet connected

Why provide internet access?

The internet is an essential for education, business and social interaction. ELA Training Services encourages the provision of quality internet access to enable learning.

ELA Training Services have content filtering and monitoring software in operation on their routers.

Internet

- ELA Training Services learners will be encouraged to tell their trainer/assessor immediately if they encounter any material that makes them feel uncomfortable.
- Internet access will be filtered appropriate to the age of the learner.

Email:

- All emails sent must be professional in tone and content.
- ELA Training Services learners must immediately tell the trainer/assessor if they receive offensive email in an ELA led training session.
- ELA Training Services learners must not reveal personal details of themselves or others in email communication (such as address or telephone number).
- ELA Training Services learners should be made aware that the writer of an email (or the author of a web page) may not be the person claimed.

How ELA Keeps you eSafe?

Hardware

All ELA laptops and desktops supplied by the company are accessible by username and password. No guest accounts are issued.

If you are issued with a Dell Machine, Dell SafeGuard and Response, powered by VMware Carbon Black and Secureworks prevents, detects & remediates cyber-attacks.Dell SafeData with Netskope and Absolute encrypts sensitive information & protects data.

Software

All ELA laptops and desktops supplied by the company run on Windows 10 which includes Windows Security, that provides the latest antivirus protection. Your device is actively protected from the moment you start Windows 10. Windows Security continually scans for malware (malicious software), viruses, and security threats. In addition to this real-time protection, updates are downloaded automatically to help keep your device safe and protect it from threats.

- Windows Security has the following tools that protect your device and your data:

- Virus & threat protection - Monitor threats to your device, run scans, and get updates to help detect the latest threats.

- Account protection - Access sign-in options and account settings, including Windows Hello and dynamic lock.

- Firewall & network protection - Manage firewall settings and monitor what's happening with your networks and internet connections.

- App & browser control - Update settings for Microsoft Defender SmartScreen to help protect your device against potentially dangerous apps, files, sites, and downloads.You'll have exploit protection and you can customize protection settings for your devices.

- Device security - Review built-in security options to help protect your device from attacks by malicious software.

- Device performance & health - View status info about your device's performance health, and keep your device clean and up to date with the latest version of Windows 10.

- Windows Security is built-in to Windows 10 and includes an antivirus program called Microsoft Defender Antivirus. (In previous versions of Windows 10, Windows Security is called Windows Defender Security Center).

- Access to the Wifi network is secured by a WPA/WPA2 - PSK [TKIP/AES] security type

- Company emails are sent using Microsoft Outlook

- Outlook encrypts email using S/MIME (Secure/Multipurpose Internet Mail Extensions) and Office 365 message encryption.

- If you receive a message that looks suspicious, or contains an attachment you're not expecting, look for the trusted sender icon and mail header. If you see this icon, the email is safe to open. If you don't see the trusted sender icon, contact the sender to verify they sent the message.

Password Best practices:

- Do not use a master password that you use everywhere (such as email, work, school, home, network)

- If possible, do not share your password with anybody.

- Passwords that are shared with others, like for a home network, should only be shared if necessary.

- Be aware when typing your password in public, or that in no way anyone is watching.

- Some types of electronic devices like computers and smartphones can remember passwords, so beware of devices that are not yours.

- Make a schedule of when to change your password. For example, every 180 days.

- It is not recommended to write down passwords. But if you have to, make sure that it is neither physically nor visually accessible by others.

Social Networking

ELA Training Services trainers/assessors shall:

- Always behave responsibly and professionally in connection with the use of social networking sites and keep up to date with privacy policies of the sites they use

- Ensure that all communication with ELA Training Services learners (including on-line communication) takes place within clear and explicit professional boundaries

- Use their professional judgment and, where no specific guidance exists, take the most prudent action possible and consult with the Director of ELA Training Services if they are unsure

- co-operate with ELA Training Services in ensuring the implementation of this policy

ELA Training Services Website :

- Website photographs that include ELA Training Services learners will be selected carefully and will only be published with permission.

- ELA Training Services learners' full names will not be used anywhere on the website, particularly in association with photographs.

Cyberbullying:

Cyberbullying is the use of the internet and related technologies to harm other people, in a deliberate, repeated, and hostile manner. When learners are the target of bullying via mobile phones, gaming or the internet, they can often feel very alone and, a once previously safe and enjoyable environment or activity, can become threatening, harmful and a source of anxiety. Cyberbullying (along with all forms of bullying) will not be tolerated. All incidents reported will be recorded and investigated.

ELA Training Services Trainer/Assessor Data Security:

- ELA Training Services trainers/assessors must not share their user account details and must not leave their computers unlocked and accessible to learners.

ELA Training Services Learners:

- All ELA Training Services learners must sign the Code of Conduct and Learner Agreement.
- E-Safety rules will be given to learners in their learner handbook.
- Any breaches of the Code of Conduct with reference to ICT will be referred directly to ELA Training Services and internet access may be denied.
- ELA Training Services Guardianship Children will be informed that network and internet use on a home stay host's computer will be monitored.

Employers' Support:

- Employers' attention will be drawn to ELA Training Services' E-Safety Policy in the parent handbook.
- Employers will be asked to read through the ELA Training Services Guardianship Learner Code of Conduct with their learner and for the learner to sign the agreement.

Policy Implementation:

- All new ELA Training Services trainers/assessors receive e-safety advice and guidance as part of their induction programme to ensure they understand their responsibilities, as detailed in this policy.

Adoption Date	Updated	Review Date	Director
08/2018	1/8/2022	1/8/2023	