Policy Number: **02-C-009**	**E-Safety Policy**
	Date of last revision: 16 May 2016
	Date of Last Review: 17 September 2018
	Date of Next Review: 17 September 2019

1.0 INTRODUCTION

Canal Engineering Ltd recognises the benefits and opportunities that new technologies offer to teaching and learning. We provide internet access to all learners and staff and encourage the use of technologies in order to enhance skills, promote achievement and enable lifelong learning. However, the accessibility and global nature of the internet and different technologies available mean that we are also aware of potential risks and challenges associated with such use, which include potential safeguarding concerns.

Our approach is to implement appropriate safeguards within the company while supporting staff and learners to identify and manage risks independently and with confidence. We believe we can achieve our aims through a combination of security measures, training, guidance and implementation of our procedures. In accordance with our duty to safeguard learners, we will do all that we can to make our learners and staff aware of the precautions they should take to be e-safe.

1.1 Scope

This procedure applies to all employees and learners of Canal Engineering Ltd and its Training Academy who have access to the company's systems, both on the premises and remotely. Any user of the company's systems must adhere to the E-mail, Telephone and Internet Policy. The E-Safety Policy applies to all use of the internet and forms of electronic communication such as email, mobile phones and social media sites.

2.0 REVISIONS

Date	Pages / Sections	Issue Status	Amendment Details
16 May 2016	All	Issue 1	First issue of procedure

3.0 ROLES & RESPONSIBILITIES

There are clear lines of responsibility for e-safety within the company. The first point of contact is the Group HR Manager who is the designated e-Safety Officer. All employees are responsible for ensuring the safety of learners and must report any concerns immediately to the e-safety officer. When informed about an e-safety incident, employees must take particular care not to guarantee any measure of confidentiality towards either the individual reporting it, or to those involved.

All learners must know what to do if they have e-safety concerns and who to talk to. In most cases, this will be the Training Academy Manager or the E-Safety Officer.   Where any report of an e-safety incident is made, all parties should know what procedure is triggered and how this will be followed up. Where management considers it appropriate, additional support may be sought from external agencies.

3.2 e-Safety Officer

The e-Safety Officer is responsible for keeping up to date with new technologies and their use, as well as attending relevant training. It is the e-Safety Officer's responsibility to review and update the e-Safety Policy, deliver staff development and training, report any developments and liaise with the local authority and external agencies as needed to promote e-safety.

3.3 Learner

Learners are responsible for using the company's IT systems and mobile devices in accordance with the E-mail, Telephone and Internet Policy. Learners must act safely and responsibly at all times when using the internet and/or mobile technologies. Learners must follow reporting procedures when they are worried or concerned, or when they believe an e-safety incident has taken place, involving them or another member of the training academy. In the first instance incidents should be reported to the training academy manager.

3.4 Employees

All staff are responsible for using company IT systems and mobile devices in accordance with the E-mail, Telephone and Internet Policy.

All digital communications with learners must be professional at all times and all online communication with learners should be carried out through the company's network and not through social media.

All staff should apply relevant college policies and understand the incident reporting procedures. Any incident that is reported to or discovered by a staff member must be reported in line with any other safe guarding incident.

4.0 SECURITY

The company will take all necessary and reasonable steps to ensure the company's network is safe and secure. Every effort will be made to keep security software up to date. The company has appropriate security measures in place; these include the use of enhanced filtering and protection of firewalls, servers, routers, work stations etc. to prevent accidental or malicious access of company systems and information.

5.0 BEHAVIOUR

The company will not tolerate any abuse of IT systems. Whether offline or online, communications by employees and learners must be courteous and respectful at all times. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the student and employee disciplinary procedures, and other relevant policies and procedures, such as the Anti-Bullying and Harassment Policy and Procedure.

Where conduct is found to be unacceptable, the company will deal with the matter internally. Where conduct is considered illegal, the company will report the matter to the police.

6.0 USE OF IMAGES AND VIDEOS

The use of images, or photographs, is popular in teaching and learning and should be encouraged where there is no breach of copyright or other rights of another person (e.g. images rights or rights associated with personal data). This will include images downloaded from the internet and those belonging to employees or learners.

The training academy teaching staff will provide information to learners on the appropriate use of images, including photographs of learners and employees as well as using third party images. Our aim is to reinforce good practice as well as to offer further information for all users on how to keep their personal information safe.

7.0 PERSONAL INFORMATION

Personal information is information about a particular living person. Canal Engineering Ltd collects and stores the personal information of learners and employees regularly e.g. names, dates of birth, email addresses, assessed materials and so on. The company will keep that information safe and secure and will not pass it onto anyone else without the express permission of the learner/employee.

No personal information can be posted to the company website/without the permission of the company's Marketing Manager. Only names and work email addresses of staff will appear on the company's website. No personal information pertaining to staff and learners will be available on the website without consent.

Employees must keep learners' personal information safe and secure at all times. Employees should only use the company's online based platforms and all personal information must be password protected. Every user of IT facilities is required to log off on completion of any activity, or where they are physically absent from a device for any period.

All company mobile devices such as a laptop or USB (containing personal data) must be password protected. Where any personal data is no longer required, it must be securely deleted in line with the Data Protection policy.

8.0 EDUCATION AND TRAINING

With the current unlimited nature of internet access, it is impossible for the Company to eliminate all risks for employees and learners. It is our view therefore that the company should support employees and learners to stay e-safe through regular training and education. This will provide individuals with skills to be able to identify risks independently and manage them effectively.

8.1 For learners

All learners will have e-safety lessons during their induction. Issues associated with e-safety apply across the curriculum and learners receive guidance on what precautions and safeguards are appropriate when making use of the internet and technologies. Learners should also know what to do and who to talk to where they have concerns about inappropriate content, either where that material is directed to them, or where it is discovered as part of a random search.

Within classes, learners will be encouraged to question the validity and reliability of materials researched, viewed or downloaded. They will also be encouraged to respect the copyright of other parties and to cite references properly.

8.2 For staff

Periodically, employees will take part in mandatory e-safety training. Any new or temporary users will receive information on the company's IT system.

9.0 INCIDENTS AND RESPONSES

Where an e-safety incident is reported to the company, this matter will be treated seriously. The company will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring. If a learner wishes to report an incident, they can do so to the training academy manager, to the e-safety officer or to any member of staff who they trust. Where a member of staff wishes to report an incident, they must contact the Human Resources team as soon as possible. Following any incident, the company will review what has happened and decide on the most appropriate and proportionate course of action, which may include recourse to other company policies and procedures such as the relevant Disciplinary Procedure. Sanctions may be put in place, external agencies may be involved and/or the matter may be resolved internally depending on the seriousness of the incident. Serious incidents will be dealt with by the Senior Leadership Team, in consultation with appropriate agencies.

10.0 MONITORING AN REVIEW

The company will monitor this policy on an annual basis, or more frequently if required, to judge its effectiveness and it will be updated in accordance with changes in the law.