E-SAFETY POLICY

JANUARY 2024

Contents

1. Introduction 2
2. Definitions 2
3. Principles 2
4. Scope and Limitations 3
5. Responsibilities 3
6. Implementation Arrangements 3
7. Procedure 3
8. Managing Director 3
9. Management Team 3
10. Employees 4
11. Senior Designated Safeguarding Person 5
12. Learners/Apprentices 5
13. Monitoring and Review 5

E-Safety Policy

1. Introduction

1.1 New technologies have become integral to the lives of learners in today's society, both within Skills Edge Training ("SET") and in their lives outside.

1.2 The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone.

1.3 These technologies can stimulate discussion, promote creativity, and increase awareness of context to promote effective learning. Learners should have an entitlement to safe internet access at all times.

1.4 The requirement to ensure that all people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in and with SET are bound.

1.5 This is also reflected in the Byron Review, which identified that alongside new technology a new culture of responsibility was needed, where all in society focus not on defending well-established positions, but on working together to help young people keep themselves safe, to help parents/guardians to keep them safe and to help each other support young people and parents/guardians in this task.

2. Definitions

2.1 E-Safety is defined as the awareness, practice, and training of individuals together with IT infrastructure security and integrity to ensure the safe use of online technologies, thus maintaining both an individual's physical and psychological wellbeing as well as organisational reputation.

3. Principles

3.1 This policy, procedure and guidelines have been produced as a framework for the protection of all in relation to e-Safety.

3.2 The education of learners in e-Safety is an essential part of SET's E-Safety provision.

3.3 Learners need the help and support of SET to recognise and avoid E-Safety risks and build their resilience.

3.4 E-Safety awareness will be provided by SET in a variety of ways, including its delivery, identified e-safety themes and through a range of external agencies.

3.5 Many parents and carers have only a limited understanding of E-Safety risks and issues, yet they play an essential role in the education of their dependents and in the monitoring/regulation of their on-line experiences.

4. Scope and Limitations

4.1 This policy applies to all employees, learners, and visitors to SET and its delivery partners who have access to and are users of ICT systems.

5. Responsibilities

5.1 The Managing Director is responsible for safeguarding and is responsible for overseeing the implementation arrangements covered by this Policy.

6. Implementation Arrangements

6.1 The roles and responsibilities of staff in implementation of this policy and procedures are set out clearly in the procedure.

6.2 All new members of staff are to be made aware of the policy and procedures during the formal staff induction process.

6.3 Updated and amended procedures will be disseminated and reinforced in training sessions, team meetings and via email communications.

7. Procedure

7.1 The following lays out the roles and procedures for E-Safety of individuals and groups within SET.

8. Managing Director

8.1 The Managing Director has overall responsibility for all matters relating to safety, including E-Safety.

8.2 This responsibility includes ensuring that management is addressed through comprehensive policies and procedures that are effectively implemented and appropriately resourced within the overall financial of SET.

9. Management Team

9.1 Members of the Management Team are responsible for ensuring that this policy is understood by all employees and fully implemented within their area(s) of responsibility.

9.2 They are responsible for ensuring that within their areas there are effective arrangements in place for the prompt reporting and management of any adverse incidents.

9.2.1. That SET's ICT infrastructure is secure and is not open to misuse or malicious attack.

9.2.2. That users may only access SET's networks through a properly enforced password protection policy, in which passwords are continually changed.

9.2.3. SET's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.

9.2.4. That SET keeps up-to-date with E-Safety technical information in order to effectively carry out its E-Safety role and to inform and update others as relevant.

9.2.5. That any concerns raised over the use of the network/remote access/email will be investigated in accordance with the SET's policy.

9.2.6. That monitoring software/systems are implemented and updated as agreed, in line with SET's policies.

10. Employees

10.1 Employees are responsible for ensuring that:

10.1.1. They have an up-to-date awareness of E-Safety matters and of the current E-Safety Policy and supporting documents.

10.1.2. They have read, understood, and signed SET's Employee Acceptable User Policy/Agreement.

10.1.3. They report any suspected misuse or problem to the appropriate person, in line with SET Policy.

10.1.4. Digital communications with students via email should only be on a professional level.

10.1.5. E-Safety issues are embedded in all aspects of the apprenticeship.

10.1.6. They monitor ICT activity in lessons and extra-curricular.

10.1.7. They are aware of E-Safety issues related to the use of mobile phones, cameras, and handheld devices and that they monitor their use.

10.1.8. In lessons where internet use is pre-planned learners are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

11. Senior Designated Safeguarding Person

11.1 A Senior Designated Safeguarding Person has day-to-day responsibility for E-Safety, and is aware of the potential for serious safeguarding issues arising from:

11.1.1. Sharing of personal data.

11.1.2. Access to illegal / inappropriate materials.

11.1.3. Inappropriate on-line contact with adults / strangers.

11.1.4. Potential or actual incidents of grooming.

11.1.5. Cyber-bullying.

12. Learners/Apprentices

12.1 Learners and apprentices:

12.1.1. Are responsible for using SET/delivery partner's systems in accordance with the laid down policies.

12.1.2. Have an understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

12.1.3. Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

12.1.4. Will be expected to know and understand SET expectations on the use of mobile phones, digital cameras, and hand-held devices. They should also know and understand SET policies on the taking / use of images and on cyber-bullying.

12.1.5. Should understand the importance of adopting good E-Safety practice when using digital technologies outside of their learning.

13. Monitoring and Review

13.1 The Managing Director will be responsible for monitoring the effectiveness of the policy.

13.2 Any serious weaknesses are to be reported to the Managing Director, who has the responsibility of ensuring the overall effectiveness of the policy.

13.3 Due to the ever-changing nature of Information and Communication Technologies, the E-Safety Policy will be reviewed annually and, if necessary, more frequently in response to any significant new developments in the use of the technologies, new threats to E-Safety, organisational or management changes or incidents that have taken place.

This Policy has been approved and authorised by:

Name: James Miller

Position: Managing Director

Date: 10 January 2024

Signature: