e-Safety Policy

Date reviewed / edited	No change / Change details	Author / Reviewer	Approved by	Next review date
V1 22.02.19	Policy issues as part of a QA review	Olanrewaju Sharafa	Theresa Mgbeobuna	March 2020

Contents

Introduction

TCFHE recognises the benefits and opportunities which new technologies offer to teaching and learning. Our approach is to implement safeguards within the College, and to support staff, tutor/assessors and learners to identify and manage risks. We believe this can be achieved through a combination of security measures, training and guidance and implementation of our associated policies. In furtherance of our duty to safeguard learners, we will do all that we can to make our learners and staff stay 'e-safe' and to satisfy our wider duty of care. This e-safety policy should be read in conjunction with other relevant College policies procedures such as Prevent and Safeguarding, IT Acceptable Use and the Harassment and Anti-Bullying Policy, and College Disciplinary Policies.

Definition of E-Safety

The term e-safety is defined for the purposes of this document as the process of limiting the risks to children, young people and vulnerable adults when using the internet, digital and mobile technologies (IDMTs) through a combined approach to policies and procedures, infrastructures and education, including training, underpinned by standards and inspection.

E-safety risks can be summarised under the following three headings.

Content

- Exposure to age-inappropriate material
- Exposure to inaccurate or misleading information
- Exposure to socially unacceptable material, such as that inciting violence, hate, extremism or intolerance
- Exposure to illegal material, such as images of child abuse
- Illegal downloading of copyrighted materials e.g. music and films

Contact

- Grooming using communication technologies, potentially leading to sexual assault or child prostitution
- Radicalisation the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups.
- Bullying via websites, mobile phones or other forms of communication device

Commerce

- Exposure of minors to inappropriate commercial advertising
- Exposure to online gambling services
- Commercial and financial scams

Scope

The policy applies to all persons who have access to College IT systems, both on premises and remote access. Any user of College IT systems must adhere to this policy and an IT Acceptable Use Policy. The e-Safety policy applies to all use of the internet, and electronic communication devices such as e-mail, mobile phones, games consoles, social networking sites, and any other systems that use the internet for connection and providing of information.

Aims

- To ensure user behaviour is safe and appropriate
- To assure that the storage and use of images and personal information on College IT-based systems is secure and meets all legal requirements
- To educate staff, tutor/assessors and learners in e-safety
- To ensure any incidents which threaten e-safety are managed appropriately

Outcomes

Security

College networks are safe and secure, with appropriate and up-to-date security measures and software in place.

Risk assessment

When making use of new technologies and online platforms, staff are to assess the potential risks that they and their learners could be exposed to

Behaviour

It is an unacceptable to download or transmit any material which might reasonably be considered obscene, abusive, sexist, racist, defamatory, related to violent extremism or terrorism or which is intended to annoy, harass or intimidate another person. This also applies to use of social media systems accessed from College systems.

- All users of technology adhere to the standards of behaviour set out in the IT Acceptable Use Policy.
- All users of IT adhere to College guidelines when using email, mobile phones, social networking sites, games consoles, chat rooms, video conferencing and web cameras, etc.
- Any abuse of IT systems and any issues of bullying or harassment (cyber bullying) are dealt with seriously, in line with staff and learner disciplinary procedures.
- Any conduct considered illegal is reported to the police.
- Staff must take responsibility for moderating any content posted online.
- Staff should be aware of cyber bullying, grooming law and child protection issues and forward any concerns to the Lead Safeguarding Manager.
- Staff should keep personal and professional lives separate online
- Staff should not have students as 'friends' on social media sites that share personal
- information.
- Staff should be wary of divulging personal details online and are advised to investigate privacy settings on sites to control what information is publicly accessible.
- Staff should recognise that they are legally liable for anything they post online.
- Staff are always expected to adhere to the college's equality and diversity policy and not post derogatory, offensive or prejudiced comments online.
- Staff should not bully or abuse colleagues/learners.
- Staff entering a debate with a learner online should ensure that their comments reflect a professional approach.
- Staff should not post any comments online that may bring the College into disrepute or that may damage the College's reputation.

- Staff wishing to debate and comment on professional issues using personal sites, should be aware that this may be seen as a reflection of College views, even with a disclaimer, and should consider their postings carefully.
- Staff should not use their College e-mail address to join sites for personal reasons or make their College e-mail address their primary contact method.
- Staff should be aware that any reports of them undertaking inappropriate online activity that links them to the College will be investigated and may result in disciplinary action.

Use of images and video

The use of images or photographs is encouraged in teaching and learning. Providing there is no breach of copyright or other rights of another person.

College staff provide information to learners on the appropriate use of images, and on how to keep their personal information safe.

Advice and approval from a senior manager are sought in specified circumstances or if there is any doubt about the publication of any materials.

Personal information

- Processing of personal information is done in compliance with the Data Protection Act 1998 and 2017 GDPR.
- Personal information is kept safe and secure and is not passed on to anyone else without the express permission of the individual.
- No personal information is posted to the College website/intranets without the permission of a senior manager.
- Staff always keep learners' personal information safe and secure.
- When using an online platform, all personal information is password protected.
- No personal information of individuals is taken offsite unless the member of staff has the permission of their manager.
- Every user of IT facilities logs off on completion of any activity, or ensures rooms are locked if unsupervised, where they are physically absent from a device.
- College mobile devices that store sensitive information are encrypted and password protected.
- Personal data no longer required, is securely deleted.

Education and Training

Staff, tutor/assessors and learners are supported through training and education to develop the skills to be able to identify risks independently and manage them effectively.

Learner inductions and the tutorial programme contains information on e-safety.

Learners are guided in e-safety across the curriculum and opportunities are taken to reinforce e-safety. Learners 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.

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

Incidents and response

A clear and effective incident reporting procedure is maintained and communicated to learners and staff.

Reports of e-safety incidents are acted upon immediately to prevent, as far as reasonably possible, any harm or further harm occurring.

Action following the report of an incident might include disciplinary action, sanctions, reports to external agencies (e.g. the police), review of internal procedures and safeguards, tutor support for affected learners, etc.

Responsibilities

The Lead or Deputy Safeguarding Manager is responsible for maintaining this policy, and for maintaining best practice in IT procedures and practices to manage any e-safety risks effectively.

The following are responsible for implementing it: -

- Lead Safeguarding Manager for all e-safety matters in relation to College staff, tutor/assessors and learners.

All tutor/assessors are responsible for embedding e-safety education and practice into their teaching programme.

All College staff are responsible for staying alert and responding appropriately to any potential or actual e-safety issue.

All College managers are responsible for implementing good e-safety practice and safeguards consistent with this policy in their area of responsibility.

Quality assurance and monitoring and review of the e-safety policy

Quality assurance activity will take place at least annually. The aim of this review is to ensure the e-safety activity is effective in safeguarding staff, tutor/assessors and learners. This is likely to be carried out during as part of a wider safeguarding review which will be scheduled and held online; MESMA-ENQUIRE.

Documents associated with this procedure

Name	Stored
Quality Assurance Enquiry Form	Use the template in MESMA-ENQUIRE