Online Safety Policy

Eat That Frog Group

INTRODUCTION

Eat That Frog C.I.C recognises the benefits and opportunities which new technologies offer to teaching and learning. Our approach is to implement safeguards within the ETFG, and to support staff and customers 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 vulnerable people, we will do all that we can to make our customers 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 ETFG policies procedures such as Safeguarding, IT Acceptable Use, Child Protection Policies, Safer Working Practices (Feb 2022). KCSIE (2022) and the Harassment and Anti - Bullying Policy, and Disciplinary Policies.

The Online Safety policy is regularly reviewed and reflects the "4Cs" (Content/Contact/Conduct/Commerce).

2. 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 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 headings.

2.1 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

2.2 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

2.2 Conduct

- Hateful Behaviour
- Harmful Behaviour
- Illegal Behaviour
- User-generated problematic Behaviour

2.3 Commerce (contract)

- Exposure of minors to inappropriate commercial advertising
- Exposure to online gambling services
- Commercial and financial scams
- Child trafficking, streaming child sexual abuse

3. Scope

The policy applies to all persons who have access to ETFG IT systems, both on premises and remote access. Any user of ETFG IT systems must adhere to e-Safety Rules and a Social Media Policy.

The e-Safety Policy applies to all use of the internet, and electronic communication devices such as email, mobile phones, games consoles, social networking sites, and any other systems that use the internet for connection and providing of information.

4. Aims

The aims are to:

- To ensure safeguards on ETFG IT-based systems are strong and reliable
- To ensure user behaviour is safe and appropriate
- To assure that the storage and use of images and personal information on ETFG IT based systems is secure and meets all legal requirements
- To educate Staff and learners in e-safety
- To ensure any incidents which threaten e-safety are managed appropriately
- Minimise inappropriate use when learners are using their own data plan

5. Outcomes

5.1 Security

ETFG networks are safe and secure, with appropriate and up-to-date security measures and software in place. This includes specialist monitoring software to respond and safeguard the welfare and well-being of digital users.

5.2 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. This risk assessment should include both when learners are accessing online learning whilst out of college.

Learners who own their own data plan should also be risk assessed as a user to minimise inappropriate use and educate the use of internet online safety.

5.3 Behaviour

- It is 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 the use of social media systems accessed from ETFG systems.
- All users of technology adhere to the standards of behaviour set out in the IT Social Media Policy.
- All users of IT adhere to ETFG 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 learners' 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 cyberbullying, 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 learners as 'friends' on social media sites that share personal information.
- Staff should be wary of divulging personal details online and are advised to look into 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 expected to adhere to the ETFG's Equality and Diversity Policy at all times and not post derogatory, offensive or prejudiced comments online.
- Staff should not bully or abuse colleagues/customers online
- Staff entering into a debate with a customer online should ensure that their comments reflect a professional approach.
- Staff should not post any comments online that may bring ETFG into disrepute or that may damage the ETFG'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 ETFG views, even with a disclaimer, and should consider their postings carefully.
- Staff should not use their ETFG e-mail address to join sites for personal reasons or make their ETFG 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 ETFG will be investigated and may result in disciplinary action.

5.4 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.
- Staff and customers are trained in the risks of downloading, posting and sharing images, and particularly in the risks involved in posting personal images onto social networking sites, for example.
- ETFG staff provide information to customers 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.

5.5 Personal information

- Processing of personal information is done in compliance with the General Data Protection Regulation 2016/679
- 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 ETFG website/intranets without the permission of a senior manager.
- Staff keep customers' personal information safe and secure at all times.
- 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.
- ETFG mobile devices that store sensitive information are encrypted and password protected.
- Personal data no longer required, is securely deleted.

5.6 Education and Training

- Staff and customers are supported through training and education to develop the skills to be able to identify risks independently and manage them effectively.
- Customer inductions and the tutorial programme contains sessions on e-safety.
- Customers are guided in e-safety across the curriculum and opportunities are taken to reinforce e-safety messages.
- Customers know what to do and whom 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, customers 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.
- Any new or temporary users receive training on the ETFG IT system. They are also asked to read, agree and sign a Social Media Policy.

6. 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.

7. Responsibilities

- The IT and Security Lead and Designated Safeguarding Lead are 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:
  - Human Resources for all e-safety matters in relation to ETFG Staff.
  - Designated Safeguarding Lead for all e-safety matters in relation to ETFG Customers.
  - The IT and Security Lead for championing good e-safety practices in ETFG IT facilities and processes, and for providing technical expertise when issues are being investigated.
  - Business Managers and all tutoring staff/mentors for providing pastoral and practical support for Post 16 learners dealing with issues related to e-safety and for incorporating e-safety in learners induction, supporting the tutorial scheme of work, and for providing an appropriate range of resources to tutors.
  - All tutors for embedding e-safety education and practice into their teaching programme.
  - All Managers for implementing good e-safety practices and safeguards consistent with this policy in their area of responsibility.
  - The Safeguarding Team for overseeing and reviewing e-safety arrangements.
  - All members of ETFG staff for staying alert to and responding appropriately to any potential or actual e-safety issue.

8. Access to the Policy

The policy is published on the BreatheHR under ‘Online Safety Policy’.

9. Monitoring and Review (effectiveness)

Eat That Frog C.I.C Safeguarding Team is made up of staff including the Safeguarding and Quality Director. The consultation was carried out via the Board of Directors before the policy was approved.

The impact of the policy will be monitored regularly with a full review being carried out at least once every year. The policy will also be reviewed where concerns are raised by the Designated Safeguarding Lead, or where an e-safety incident has been recorded.

Staff are trained on all aspects of e-safety. Staff are also asked to adhere to a Social Media Guide.

10. Legal and other Frameworks

- Working together to safeguard children (HM Government) July 2018 (updated July 2022)
- Keeping children safe in education (DfE) September 2022
- The Prevent Duty (HM Government) April 2021
- Channel Duty Guidance (HM Government) April 2020
- Inspecting safeguarding in early years, education and skills settings (Ofsted) August 2021
- The Education (Independent School Standards) Regulations (2014)
- The Equality Act (2010)
- The Human Rights Act 1998
- Searching, screening and confiscation in schools (September 2022)
- Sexting in Schools and Colleges (UK Council for Child Internet Safety)

Related Documents

Eat That Frog C.I.C Safeguarding Technical Security Statement IT Security Policy Related Forms:

- Staff Reporting Form for e-safety incidents
- Staff Social Media Policy.

Additional Support

The following websites are extremely helpful when dealing with cyberbullying and e-safety issues;

- CEOP - www.ceop.police.uk - Child Exploitation and on-line Protection Centre
- Bullying Online - www.bullying.co.uk - Advice for children, parents and colleges
- Virtual College - www.safeguardingchildrenea.co.uk
- Kidsmart - www.kidsmart.org.uk - An Internet safety site from Childnet, with low-cost leaflets for parents.
- Think U Know? www.thinkuknow.co.uk Home Office site for learners and parents explaining Internet dangers and how to stay in control.
- Safekids www.safekids.com Family guide to making the Internet safe, fun and productive
- Maths Doctor www.mathsdoctor.co.uk/online/child-safety - How To Keep Your Child Safe Online
- UK Safer Internet www.saferinternet.org.uk

Online Safety Policy

Date	Page	Details of the change	Agreed by
Dec21	All	Reviewed – no change	Board
1/09/22	All	Changes to reflect KCSIE and Working together updates etc	Board
05/04/23	1	Removed the word 'three' from: "E-safety risks can be summarised under the following **three** headings".	
Next review April 2024			