E-Safety & Acceptable Use Policy

Introduction

Friends Centre recognises the benefits and opportunities which new technologies offer to teaching and learning.

We provide free internet access at both our sites to all learners to 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.

Friends Centre recognises the benefits and opportunities which new technologies offer to teaching and learning.

Purpose

We provide free internet access at both our sites to all learners to 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. Our approach is to implement appropriate safeguards while supporting learners to identify and manage risks independently and with confidence. We believe this can be achieved through a combination of security measures, guidance and implementation of our policies. We monitor PC usage and/or block specific sites relating to pornography, violent extremism or any sites of a radical nature. To safeguard learners we will do all that we can to make them stay e-safe and to satisfy our wider duty of care.

The policy applies to all learners of Friends Centre who have access to our IT systems (including our Virtual Learning Environment (VLE) and mobile devices, both on the premises and remotely. Any user must adhere to a Learning Agreement which entails agreeing to abide by our rules for our IT Acceptable Use Policy if they are using our IT systems.

The E-Safety Policy applies to all use of the internet and forms of electronic communication such as email, mobile devices, VLE and social media sites.

This e-safety policy should be read alongside other relevant policies e.g. Data Protection, Equality and Diversity, IT Acceptable Use, Learner Management and Safeguarding and Prevent Duty.

Responsibilities

The following staff are responsible for implementing this policy:-

- The E-Safety Officer (Centre Manager) for ensuring that new technology is kept up to date
- Principal and Lead Tutors for ensuring relevant training is attended by relevant staff, supporting the tutorial scheme of work and providing an appropriate range of resources to tutors

- Tutors for providing pastoral and practical support for learners dealing with issues related to e-Safety and incorporating e-safety in student induction
- Reception staff for maintaining records from Classlink and/or dealing with white listing/black listing according to Open DNS systems

The Centre Manager (Safeguarding Officer) who also acts as the e-Safety Officer, Safeguarding Trustee and Principal are responsible for the maintenance, regular review and updating of this policy. The Senior Management Team and Curriculum Team will be consulted on any changes, which will be agreed by the Board of Trustees, who may also request a review of the policy when issues are identified.

The Principal is responsible for the implementation of an effective E-Safety & Acceptable Use Policy and this policy is endorsed by the Quality Improvement Group who recommend its approval to the Board of Trustees. The policy is reviewed by the Centre Manager on an annual basis and any amendments approved by the Board of Trustees on the recommendation of the Quality Improvement Group. Management staff and tutors are designated to implement aspects of the policy relevant to their roles.

Definition of E-Safety

The term E-safety is defined for the purposes of this document as the process of limiting the risks to 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 inciting violence, hate, intolerance or radicalisation
- 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 and/or child prostitution/radicalisation
- bullying via websites, mobile phones or other forms of communication devices

Commerce

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

Acceptable Use

Learners are responsible for using our IT systems, VLE and mobile devices in accordance with this Policy. They agree to these terms by signing a Learner Agreement at Induction and on registering to use our public access computers. Learners must act safely and responsibly at all times when using the internet and/or mobile technologies. They must follow reporting procedures where they are worried or concerned, or where they believe an e-safety incident has taken place involving them or another learner.

Friends Centre will not tolerate any abuse of IT systems. Whether offline or online, communications by learners should be courteous and respectful at all times. Any reported incident of bullying, harassment, messages of violent extremism or other unacceptable conduct will be treated seriously and in line with learner disciplinary codes. *For further information see our Learner Management Policy, IT Acceptable Use Policy and Safeguarding and Prevent Duty Policy.*

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

Users must not view websites that could be considered adult or pornographic, obscene or contain indecent material, contain violent extremism messages or videos of violence with messages of “glorification” or praise for those with extreme views. Friends Centre reserves the right to decide whether or not a website is inappropriate. If you are unsure about a website you wish to visit please ask at reception. Game playing and streaming films will not be tolerated on PCs as these facilities are prioritised for the use of improving IT skills, job searching (finding out about work or voluntary work), CV writing, letter writing, emailing and keeping in contact with people, surfing useful sites.

Users must only use their own account. Users may not give their log-ins and passwords to other people. Users should always log off after use

Users must not publish defamatory and/or knowingly false material about their colleagues, friends or about Friends Centre or it’s students/clients on social networking sites, (Facebook, Twitter etc) ‘blogs’ (online journals) and any other online publishing format

Users must not publish postings inciting people to commit acts of an extreme nature or calling for racial or religious violence

Users must not try to alter Friends Centre software or try to hack into or damage the computers

Users must treat Friends Centre staff and all other users with respect at all times. Any rudeness and/or aggression towards staff or other users will NOT be tolerated
Users bringing children (under 16) must supervise them at all times and children should not use the computers

Computer use is continuously monitored for the prevention and detection of crime. If we suspect a user is breaking the guidelines above, we will block your account. You can then discuss this incident with our Support Officers who will decide if you can continue to use our computers. If you disagree with this decision, your case will be referred to the Centre Manager for further discussion.

Secure Systems

Friends Centre will do all that it can to make sure the network is safe and secure creating a safe ICT learning environment. Every effort will be made to keep security software (AVG) up to date. Appropriate security measures will include the protection of firewalls, servers, routers, work stations etc. to prevent accidental or malicious access of systems and information.

Friends Centre will ensure that all users of technologies adhere to the standard of behaviour as set out in the IT Acceptable Use Policy.

Reporting Incidents

If staff suspect an e-safety incident may have taken place i.e. the suspicion of or finding of unsuitable material/illegal material/unsuitable activity/illegal activity or suspected on a PC/Laptop/mobile device, they will immediately report this to the Centre Manager.

All staff are responsible for ensuring the safety of learners and should report any concerns immediately to their line manager. All tutors are required to be aware of e-safety issues. When informed about an e-safety incident, staff members must take particular care not to guarantee any measure of confidentiality towards either the individual reporting it, or to those involved, it should be treated as a safeguarding issue and a safeguarding incident form completed and passed on to the Safeguarding Officer.

All staff will ensure that learners know what to do if they have e-safety concerns and who to talk to. In most cases, this will be their tutor or the Centre Manager (E-Safety Officer). All PC users should report e-safety issues to our Receptions where this can be passed on. Information is displayed on pinboards and in the learner handbook signposting users with issues. Where any report of an e-safety incident is made, all parties should know the procedures and actions to be taken. Where management considers it appropriate, intervention may be required from external agencies.

Related Friends Centre Policies

Learner Management Policy
Safeguarding and Prevent Duty Policy

Related Legislation

- Racial & Religious Hatred Act 2006
- Sexual Offences Act 2003
- Police & Justice Act 2006
- Computer Misuse Act 1990 (s1-3)
- Communications Act 2003 (s127)
- Data Protection Act 1998
- Malicious Communications Act 1988 (s1)
- Copyright, Design & Patents Act 1988
- Public Order Act 1986 (s17-29)
- Protection of Children Act 1978 (s1)
- Obscene Publications Act 1959 & 1964
- Protection from Harassment Act 1997
- Regulatory of Investigatory Powers Act 2000

Review of Policy

Policy Reviewed by: (Role Title)	Date Reviewed:	Date Approved by Board of Trustees:	Next Review Date:
Interim Principal & Centre Manager	February 2015		
Centre Manager, Safeguarding Trustee & Principal	June 2016	September 2016	June 2017