Esafety Policy

1. Introduction

This policy has been created to inform employees and volunteers of Escape Arts of the expected behaviour when using email, social media and internet facilities.

Escape Arts encouraged staff and participants to make appropriate use of technologies. Escape Arts is committed to embracing new learning pathways and technologies. However, it is also important that we balance this with our duties of care to our participants and staff regardless of race, gender, religion or belief, sexual orientation, age, social economic and human rights and be particularly mindful of vulnerable groups.

Internet and email have become integral to the way Escape Arts conducts its business and should be seen as a powerful resource for employees/ volunteers to effectively perform their role. The internet provides fast and extensive access to information and, if used responsibly, can be a very useful tool for both business and personal use; email similarly provides a fast and efficient means of communication.

Escape Arts is committed to ensuring that all staff and participants, including children and young people within its remit of care will be able to use existing and well as up and coming technologies safely. Escape Arts expects its employees to conduct themselves in an exemplary manner. Employees must not act in a way which conflicts with the interests of the charity or brings Escape Arts into disrepute. Employees must apply high standards of integrity in their use of Escape Arts internet and email facilities.

With the ever-changing realm of social media, it is vital that you understand all developments, in this area to ensure that all those who work with children and young people as well as their parents are informed as to the dangers that exist so that they can take an active part in safeguarding children and young people. The aim of this policy is to give you the information you need to protect both Escape Arts and yourself.

Our approach is to implement safeguards within the organisation and to support staff and participants to identify and manage risks independently. We believe this can be achieved through a combination of security measures, training and guidance and implementation of our policies.

Definitions

The term ‘social media’ describes the set of online tools that enable shared community experience both online and in person. For the purposes of this document, internet usage means any connection to the Internet via web browsing, external email, news groups or messaging services, mobile technologies e.g. mobile phone, including bluetooth applications, PDA’s etc.

Policy Scope

The Policy applies to:

- All Escape project activities supporting children, young people, adults and families.
- All areas of staff training, planning and delivery.
- All areas supporting volunteering, fundraising and community events.

This policy applies to all members of the organisation who have access to Escape's IT systems both on the premises and remotely. The Policy applies to all use of the internet and electronic communication devices. .

Using Email and the Internet

- All employees, given email and internet access, must be made aware of this Policy (electronically or hardcopy) either via induction or informed through their Line Manager.
- Only Escape Arts employees and designated volunteers and other authorised personnel (defined in the Scope of this policy) can use the Escape Arts email and internet facilities.
- Escape Arts may withdraw a user's email and internet access rights, where it considers it appropriate to do so.
- Occasional personal use of email and internet is permitted provided that:
    - It does not interfere with the performance of the employee's duties
    - It does not incur additional costs for Escape Arts nor interfere with the running of its business
    - It is not used to access, retain or distribute material of an illegal, sexual, discriminatory or inappropriate nature.
    - It is not used in connection with any private commercial business or any activity which conflicts with the interests of Escape Arts.
    - It is not used in a way which breaches Escape Arts misconduct, equal opportunities or safeguarding policies and procedures.
    - It does not bring the Escape Arts into disrepute.
    - Employees should recognise that personal use of the internet and email, during their own normal working time, should not impact their productivity or expected working pattern.

Escape Arts expects employees to recognise that the email and internet facilities are provided, primarily, for business use. What constitutes occasional personal use will depend on the particular context in which use takes place and employees should always seek clarification from their managers, especially if there is any doubt about this issue. Employees should also be aware that they may be required to justify the extent of their personal use to their managers.

Escape Arts does not tolerate the viewing, downloading or distribution of media of an illegal, sexual, discriminatory or inappropriate nature and such behaviour may be considered to be an act of gross misconduct which may lead to dismissal.

Media can include still images, photographs, cartoons, video clips, written words or sound recordings. Examples of inappropriate material would be that of a sexual nature, images of

nudity, use of inappropriate language including swear words, violent images or other material which could be considered discriminatory or exploitative.

What may be acceptable to one employee may not be acceptable to other colleagues and as such, if employees are in any doubt whether some material is acceptable in the workplace, then they should not view or distribute that material. If employees accidentally encounter any material of this nature they must inform their Manager as soon as possible.

- Any email you send that causes damage to the Charity, any of its employees or any third parties' reputation may amount to misconduct or gross misconduct to which the Charity's Dismissal and Disciplinary Policies apply.
- Employees' usage of email, and the internet is monitored by or on behalf of the Escape Arts.
- You must not Impersonate any other person when using email.

Security

Escape will do all that it can to make sure the organisation's IT systems and future media networks are safe and secure. Every effort will be made to keep security software up to date. Appropriate measures will include the use of enhanced filtering and protection of firewalls, servers, routers, work stations to prevent accidental or malicious access of Escape systems and information.

All computers will be password protected with agreed project administrators. Passwords must not be share with participants under any circumstances. All staff will need to sign the Staff Acceptable Use Agreement in order to have administrator access (Appendix 2).

Using Social Media

Whether or not an individual chooses to create or participate in an online social network or any other form of online publishing or discussion is his or her own business. The views and opinions you express are your own.

As an Escape Arts employee it is important to be aware that posting information or views about Escape Arts can't be isolated from your working life. Any information published online can, if unprotected, be accessed around the world within seconds and will be available for all to see and will contribute to your overall Online Digital Footprint, added to whenever you use internet-based services.

Staff members must keep their own profile private including hiding their personal email address and telephone number from any participant. **Under no circumstances should Escape staff befriend project young people via a private Facebook of social media group.**

Remember you are personally responsible for any content you publish.

Understand your online privacy settings – Check your settings and understand who can see the information you publish and your personal information. Do not let your use of social media interfere with your job and always access in your own time unless this is a Escape Arts social media account.

Escape Arts Social Media Accounts:

- must not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claims for damages. This includes but is not limited to material of an illegal, sexual or inappropriate nature that may bring Escape Arts into disrepute or damage the reputation of the organisation.
- must not be used for the promotion of personal financial interests, commercial ventures or personal campaigns
- must not be used in an abusive or hateful manner
- must not breach the Escape Arts equal opportunities, safeguarding, child protection, vulnerable adult protection and confidentiality policy

The E-Safety Officer (Karen Williams) and E-Safety Trustee (Dan Senter) must be informed in writing of any social media groups or Escape related externally hosted sites being set up.

Any decision to dismiss an employee for alleged social media misconduct should be based on a fair and unbiased consideration and assessment of these factors,

If you identify yourself as working for, or a representative of, Escape Arts on any social media or internet presence, that isn't directly controlled and authorised by Escape Arts, then you have a responsibility to carry the spirit of this policy into your personal life.

Failure to comply with the Policy is a disciplinary offence and may also result in legal claims against you and the organisation. A breach of any part of this Policy may be regarded as misconduct to which Escape Arts Dismissal and Disciplinary Procedure applies and a serious breach of any part of this Code may be regarded as gross misconduct and may lead to dismissal and may also result in legal claims against you and the Escape Arts.

The creator of the group can allocate specific staff members of the group admin status allowing them the ability to remove any inappropriate content. The creator of the group must allocate admin status to the E-Safety Officer. Participants and Young People should not be given admin status.

Behaviour

Escape will not tolerate any abuse of IT systems. Whether offline or online, communication by staff and participants should be courteous and respectful at all times. Any reported incident of bullying or harassment or any other unacceptable conduct or bringing Escape into disrepute will be treated seriously and in line with the Behaviour Policy and Staff Disciplinary Policies.

The same ethical obligations that staff adhere to professionally also apply to their conduct in an online environment. They must adhere to their contract of employment.

Incidents which appear to involve deliberate access to websites, newsgroups and online groups that contain the following material will be reported to the designated officer for child protection – Karen Williams and the Police:

- Indecent images inclusive of abuse (images of children whether they are digital or cartoons, apparently under 18 years old, involved in sexual activity or posed to be sexually provocative)

- Adult material that potentially breaches the Obscene Publications Act in the UK
- Criminally racist or anti-religious material
- Violence and bomb making
- Illegal taking or promotion of drugs
- Software piracy
- Other criminal activity

In addition, participants may not use the Escape facilities (connectivity and services) or an equivalent:

- For running a private business.
- Entering into any personal transaction that involves Escape in any way;
- Visiting sites that might be defamatory or incur liability on the part of Escape or adversely impact on the image of Escape.
- Uploading, downloading, or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials belonging to third parties outside of Escape.
- Reveal or publicise confidential information, which includes but is not limited to: financial information, personal information, databases and the information contained therein, computer/network access codes and business relationships.
- Intentionally interfere with the normal operation of the Internet connection, including the propagation of computer viruses and sustained high volume network traffic (sending or receiving of large files or sending and receiving of large numbers of small files or any activity that causes network congestion) that substantially hinders others in their use of the Internet.
- To use the Internet for soliciting, representing personal opinions or revealing confidential information or in any other way that could reasonably be considered inappropriate.
- To deliberate activities with any of the following characteristics: wasting staff effort or networked resources; corrupting or destroying other users' data; violating the privacy of other users; disrupting the work of other users; continuing to use an item of networking software or hardware after Escape has requested that use cease because it is causing disruption to the correct functioning of Escape or other misuse of the Escape network, such as introduction of viruses.
- Use mobile technologies 3G or mobile internet services in any way to intimidate, threaten or cause harm to others. Moreover, mobile technologies should not be used to access inappropriate materials or encourage activities that are dangerous or illegal.

Communications

Escape advises personal invitations from staff to participants (or vice versa) should not be encouraged. No initiation or acceptance of invitations from participants within the project under the age of 18 will be sanctioned.

Staff should only use their Escape email account and not share their personal email addresses with participants. **Staff email accounts will be accessible remotely, whilst away from Escape premises.**

Staff should not disclose confidential information relating to their employment at Escape.

Sites should not be used for accessing or sharing illegal content.

If you have an Escape mobile on no account are you to ring chat lines, premium rate numbers, or numbers which relate to offensive, illegal or immoral purposes.

The sending of inappropriate text messages between any members of the Escape community is not permitted.

Use of images and videos
The use of videos and images is encouraged where there is no breach of copyright or other rights of another person.

Film and photography consent must be obtained from all staff and participants before images/videos can be taken, copied, downloaded, shared or distributed online. Please see participant's registration form.

Personal information
Escape keeps and processes certain information about its employees, participants and other users in compliance with the Data Protection Act 1988.

Any information that is stored on any removable media by staff, including laptops/PCs (both personal equipment and work equipment) that holds personal details of participants or staff must be password protected.

Any computer with the Escape database on must be password protected and accessed by staff only. Access to the database must also be secondary password protected.

Education and training
With the current unlimited nature of internet access, it is impossible for Escape to eliminate all risks for staff and participants. It is our view therefore, that Escape should support staff and students through training. This will provide them with the skills to identify risks independently and manage them effectively.

Staff will be trained by the E-Safety Officer or be expected to undertake organised e-safety training and responsible for delivering an e safety lesson to participants using technology. New staff will receive and sign the Acceptable Use Policy as part of their induction. All staff will be made aware of the Child Protection and Safeguarding Policy and Procedures and understand what to do in the event of a disclosure by a participant, including the misuse of technology.
Participants using technologies will also be required to attend an e-safety lesson delivered by the trained project lead. Within this session staff and participants are also told where they can go and who they can talk to if they have concerns about inappropriate material or other e safety concerns.

Within workshops, participants 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.

E-Safety When working with Young People
Escape will seek to ensure that across the organisation the following elements will be in place as part of its safeguarding responsibilities to children and young people by:

- Establishing a list of authorised person(s) dealing with child protection issues and E-safety in each project location.
- Establishing key internet administrators who are responsible to monitor the social media sites.
- Implementing training sessions with all young people on e-safety, including the signing of Acceptable Use Agreement.
- Provide information to parents that highlight safe practice when using the internet and other digital technologies in the project and at home.
- Provide adequate training for staff and volunteers, including in all induction.
- Provide adequate supervision of children and young people when using the internet and digital technologies.
    - Provide good role models in acceptable use of mobile phones within projects.
    - Provide up to date photography/filming parental consent forms, which are completed before publication.
- Establish a reporting procedure for abuse and misuse by children, young people and adults.
- Not sharing personal profiles with young people.
- Use of Internet facilities, mobile and digital technologies
- Participants and Staff shall not visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
    - Indecent images of children
    - Promoting discrimination of any kind
    - Promoting racial or religious hatred
    - Promoting illegal acts
    - Any other information which may be offensive to peers or colleagues e.g. abusive images; promotion of violence; gambling; criminally racist or religious hatred material.

Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for instance, illegal Internet use or child protection concerns.

Declaration
On behalf of Escape Arts, we, the undersigned, will oversee the implementation of the E-Safety Policy and take all necessary steps to ensure it is adhered to.

Responsible People:
Esafety Officer – Karen Williams
Esafety Trustee – Dan Senter

This policy and procedure was adopted: 23rd October 2018
Date for review: Oct 2020