Your fastest way to learn. Why wait?

FIREBRAND

E Safety Statement of Intent

Firebrand

Introduction

Firebrand recognises e-safety issues and the potential harm and risks it can pose to young people. All partner agencies, stakeholders, and educational settings and all other organisations within the community providing services to young people have a duty to understand e-safety issues as part of its wider safeguarding duties;

- Recognising their role in helping young people to remain safe online whilst also supporting staff
- Acknowledges that its role is strategic rather than operational as it is for partner agencies to develop and embed their own operational policies and procedures, and lines of accountability, in safeguarding young people when using Internet, Digital and Mobile Technologies (IDMT).

The term e-safety is defined for the purposes of this document as the process of limiting the risks to young people 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.

Our vision is:

- That all young people, staff and all those working with young people recognise the risks, dangers and potential harm that may arise from the use of Internet Digital and Mobile Technologies
- That they understand how to mitigate these risks and potential dangers and are able to recognise, challenge and respond appropriately to any e-safety concerns so that young people and staff are kept safe.

Background

Each new technology introduces new opportunities and challenges for young people, parents, carers and those working with young people. In order to minimise the risks involved from new technologies we need to understand how young people use IDMT and how this may be misused by those who may present a risk to young people. It is important that we know how to respond when concerns arise

In recent years, the internet and other means of electronic communications have become increasingly accessible to young people. This provides great opportunities for young people in terms of education, information, communication and having fun. The internet and social media platforms also includes risks from those intent on sexually exploiting young people and from the inappropriate use of communications technology. This highlights the need to educate young people about the benefits, risks and responsibilities of using information technology. It also highlights the need to provide appropriate guidance to those working with young people.
Local Safeguarding Children Boards have an important role in co-coordinating and ensuring the effectiveness of local work to safeguard and promote the welfare of young people. This document aims to support organisations in reviewing their own e-safety agenda and to help in developing effective e-safety policies and procedures.

Stakeholders

Statutory and voluntary organisations that young people and families may use should consider having an e-safety policy. These include community groups and private sector organisations also. This document aims to provide information for organisations in helping them to develop e-safety policies.

Objectives

All organisations that work with young people need to have an e-policy in place based on the following objectives:

1. **Ensuring** that all learners should be equipped with the knowledge and skills to safeguard themselves in the online/digital world.
2. **Ensuring** that all people who work with young people have access to effective policies and procedures and effective training to safeguard young people at risk through online activity.

3. **Ensuring** that professionals know how to respond when concerns arise regarding the misuse of communications technology.

Staff Engagement

- All staff with responsibility for young people's learning via IDMT must be familiar with the accompanying e-Safety policy and given opportunities to raise issues and concerns they face in their day to day working responsibilities.
- All staff must understand that misuse of IDMT will result in disciplinary action being taken against them in line with your organisations policies and procedures.
- Employees unsure of what constitutes acceptable usage of the internet should always check with management. They should be aware that all internet usage is monitored and can be traced back to each individual user.
- Staff must also be aware of what is acceptable in terms of their engagement with young people via IDMT means
- Staff (including volunteers) should never disclose or share their personal details except in certain exceptional roles (i.e. personal mobile phone numbers, email addresses or social networking profiles etc.) or send or accept friend requests on social networking websites with children and young people / service users.

Any necessary contact between a young person and a professional should be made via equipment and contact details provided by the employer (not personal equipment / contact details) and be clearly recorded on a need to communicate basis and with the consent of the parent/ carer or foster carer. Alternatively, personal contact details for children / young people should be stored centrally by management and only accessed on a need to know basis as approved by management.

- Organisations should adopt an open culture of vigilance in the workplace and staff must feel confident in identifying and challenging poor and/or risky working practices.
- Ideally, training on acceptable usage and responsible e-safety should be provided during the induction period for all new employees with a specific emphasis on professional boundaries, confidentiality and data protection.
- This section will help staff determine what action they can take when they identify concerns and should be read in conjunction with policy and procedures.

Protect Yourself from Cyberbullying:

- **Limit where your personal information:** Be careful who can access contact information or details about your interests, habits or employment to reduce your exposure to bullies that you do not know. This may limit your risk of becoming a victim and may make it easier to identify the bully if you are victimised.

- **Avoid escalating the situation:** Responding with hostility is likely to provoke a bully. Depending on the circumstances, consider ignoring the issue. Often, bullies thrive on the reaction of their victims. If you receive unwanted email messages, consider changing your email address. The problem may stop. If you continue to get messages at the new account, you may have a strong case for legal action.

- **Document cyberbullying:** Keep a record of any online activity (emails, web pages, social media posts, etc.), including relevant dates and times. Keep both an electronic version and a printed copy.

- **Report cyber bullying to the appropriate authorities:** If you are being harassed or threatened, report the activity to the local authorities. There is a distinction between free speech and punishable offenses. Police can help sort out legal implications. It may also be appropriate to report it to your facilitator who have separate policies for dealing with activity that involves safeguarding you and your information.

STOP. THINK. CONNECT.

- **Own your online presence:** When available, set the privacy and security settings on websites to your comfort level for information sharing. It's OK to limit how and with whom you share information.

- **Safer for me, more secure for all:** What you do online has the potential to affect everyone – at home, at work and around the world. Practicing good online habits benefits the global digital community.

- **Post only about others as you have them post about you.**

Further information:

- Computer Misuse Act 1990 (including hacking, denial of service attacks)
  http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm
- GDPR
  https://www.eugdpr.org/
- Privacy and Electronic Communications (EC Directive) Regulations 2003(including spam)
  http://www.opsi.gov.uk/si/si2003/20032426.htm
- Protection from Harassment Act 1997 (including harassment, bullying, and cyber stalking)
  http://www.opsi.gov.uk/acts/acts1997/1997040.htm