e-SAFETY POLICY

February 2024

Date of Approval	Designated Safeguarding Lead	Safeguarding Trustee	Review Date
01/02/2024	Andrew Quartermain, CEO	Priscilla Turner	01/01/2025

1.0   INTRODUCTION

As part of the Every Child Matters agenda set out by the government, the Education Act 2002 and the Children's Act 2004, it is the duty of all organisations to ensure that course participants and young people are protected from potential harm both within and beyond the organisation environment. Therefore, the involvement of course participants, young people and parent/carers is also vital to the successful use of online technologies.

2.0   AIMS

This policy aims to explain how parents/carers, course participants or young people can be a part of these safeguarding procedures. It also details how course participants and young people are educated to be safe and responsible users capable of making good judgements about what they see, find and use. The term 'e-Safety' is used to encompass the safe use of all technologies in order to protect course participants, young people and adults from potential and known risks.

• To emphasise the need to educate staff, course participants and young people about the pros and cons of using new technologies both within and outside the organisation.

• To provide safeguards and agreement for acceptable use to guide all users, whether staff or course participants and young people, in their online experiences.

• To ensure adults are clear about procedures for misuse of any technologies both within and beyond the boundaries of the organisation.

• To develop links with parents/carers and the wider community ensuring input into policies and procedures with continued awareness of the benefits and potential issues related to technologies.

3.0   WHAT ARE THE RISKS?

There are many potential risks for course participants and young people including:

• Accessing age inappropriate or illegal websites.
• Receiving unwanted or upsetting text or e-mail messages or images.
• Being "groomed" by an adult with a view to meeting the child or young person for their own illegal purposes including sex, drugs, or crime.
• Viewing or receiving socially unacceptable material such as inciting hatred or violence.
• Sending bullying messages or posting malicious details about others.
• Ignoring copyright law by downloading music, video or even homework cheat material.

WHAT ELSE MIGHT BE OF CONCERN?

A child or young person who:

• Is becoming secretive about where they are going to or who they are meeting.
• Will not let you see what they are accessing on-line.
• Using a webcam in a closed area, away from other people.
• Accessing the web or using a mobile or tablet for long periods and at all hours.
• Clears the computer history every time they use it.
• Receives unexpected money or gifts from people you don't know.

 An adult who:

• Befriends a child/ren or young person/people on the internet or by text messaging.
• Has links to course participants or young people on their Facebook or other social network site; especially if they work in a position of trust such as a sports coach or youth worker.
• Is secretive about what they are doing and who they are meeting.

4.0   MINIMISING THE RISKS:

We will:

• Talk to course participants and young people about what they are accessing online.
• Keep the computer/s in a general space where we can monitor what is going on.
• Explain the risks of giving out personal details online.
• Talk about how people can be anyone they want to be online: by using misleading emails, photographs of other people, telling lies about their age, school, hobbies.
• Encourage course participants and young people to think carefully about which photographs or videos they use online this material can be used and tampered with by other people, or they may not be appropriate.
• Advise course participants and young people to only text, chat or webcam to people they know for real.
• Talk about how to identify SPAM/SPIM messages or junk mail and how to delete them. This also applies to messages from people they do not know, or opening attachments.
• Discuss how people hide their identities online and the importance of never meeting new online "friends" for real.
• Make sure course participants and young people understand they can talk to us or their parents and/or carers about anything that makes them feel uncomfortable.
• Look on the internet together for information about how to deal with, or report, problems.
• Talk about how, when information or images get onto the net, they can never be erased or retrieved.

5.0 WHAT DO I DO IF I AM CONCERNED?

If you have any concerns speak to the lead or deputy person for e-Safety immediately.

REMEMBER:

1. DO NOT DELAY.

2. DO NOT INVESTIGATE.

3. ISOLATE ANY EQUIPMENT AND PREVENT FURTHER USE OF AN ONLINE ACCOUNT.

4. MAKE CAREFUL RECORDING OF ANYTHING YOU OBSERVE OR ARE TOLD.

5. SEEK ADVICE FROM THE LEAD OR DEPUTY PERSON FOR e- SAFETY.

6. REFER IMMEDIATELY.

6.0 CONTACTS FOR REFERRING

If the concern is about:

• A child being in imminent danger, ALWAYS DIAL 999 FOR THE POLICE.

• The welfare of a child, ring the local children's social care services- Customer First: 0808 800 4005, out of hours service: 01473 299669 or access what to do by going to www.suffolksp.org.uk

• A known person's sexual behaviour or intentions ring the local children's social care services.

• A person who has a "duty of care" in the organisation, ring the local children's social care services. The LADO (Lead Authority Designated Officer) will oversee and advise upon any following procedures.

• An unknown person's sexual behaviour or intentions, report at www.ceop.police.uk/ (Child Exploitation and Online Protection Centre).

• Harmful content, including child sexual abuse images or incitement to racial hatred content contact www.iwf.org.uk

7.0 Our e-SAFETY CODE OF CONDUCT

We expect everyone in our organisation to agree and sign up to our code of conduct: I will:

1. Use the internet and other forms of communication in a sensible and polite way.

2. Only access websites, social media, send messages or images, or access and use other resources that will not hurt or upset anybody.

3. Seek permission if I want to use personal information or take photographs of other people.

4. Report any concerns to the Designated Safety Lead or deputy immediately.

5. Be clear that I cannot maintain confidentiality if there is a concern about the welfare of a child or young person.

8.0   RESOURCES

The organisation:

• Can use the Childnet International 'KnowITAll for Parents' CD/online materials (https://www.childnet.com/resources) to deliver key messages and raise awareness for parents/carers and the community.

• Ensure that skills around internet use are offered as part of the follow-up training for parents/carers so they know how to use the tools their children and young people are using.

• Endeavour to provide access to the internet for parents/carers so that appropriate advice and information can be accessed where there may be no internet at home, subject to arrangement.

PLEASE ENSURE YOU NOW READ THE E-SAFETY FLOW CHART ON THE PAGE BELOW

APPENDIX   e-Safety Incident Flow Chart

e-Safety Incident Flowchart

Unsuitable material/illegal material/unsuitable activity/illegal activity found or suspected

Identify those involved if known, without compromising any potential evidence (staff, child, young person, vulnerable adult or unknown and whether they are a victim or investigator)

Isolate any PC/equipment as potential evidence and if appropriate arrange suspension of user account to allow investigation to be carried out

Report to local e-Safety Lead and/or e-Safety Officer and/or SDP

Is there a child protection concern? —No— **Is it an adult safeguarding concern?**

Yes / Yes

Report as appropriate to:
Customer First, LADO, Police
IWF (Internet Watch Foundation – www.iwf.org.uk)
CEOP (www.ceop.police.uk)

—No—

Is illegal or unsuitable material or activity found or suspected?

Yes / No

Allow Police or relevant organisation to complete their investigations, seeking LADO advice on treatment of victim/instigator and possible referral to ISA

Review incident, agree and Implement appropriate actions
Possible actions:
Inform parents/carers, Risk assessment
Counselling, Referral to other agency
Community resolution, Disciplinary procedures

Is illegal or unsuitable material or activity confirmed? —No—

Debrief all relevant parties at end of e-safety incident

Yes

Review policies and procedures

Police or relevant organisation take action

Organise knowledge share session

If you believe a child, young person or vulnerable adult is at risk or in immediate danger: call the Police on 999 or by clicking the CEOP report abuse button below. Immediately isolate equipment to avoid evidence tampering.

e-safety contact email:
esafer@suffolk.gov.uk
website address:
www.esafersuffolk.org

CLICK CEOP Internet Safety