



# ONLINE SAFETY POLICY

Policy Title	Online Safety Policy
Issue Date	March 2026
Review Date	March 2027
Author	Karen Double
Agreed by	Board of Trustees

# Online Safety Policy

## Introduction

Modern digital technology has made access to information and communication increasingly easy for everyone. This is especially so for those who cannot always go out to socialise and rely on websites for social networking, watching films, downloading music, buying lottery tickets, shopping etc. Government guidance is clear, that all organisations working with children, young people adults at risk, families, parents and carers have responsibilities. It is also important to remember, children, young people and adults at risk can also abuse and such incidents fall into the remit of this policy.

## Aims

This policy aims to explain how parents/carers, children or young people can be a part of these safeguarding procedures. It also details how children 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 children, young people and adults from potential and known risks. Whilst attendees do not have access to online content at LEAPS Suffolk, staff use every opportunity to educate attendees on how to use and access the internet safely.

- To emphasise the need to educate staff, children 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 children 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.
- To report and record any concerns and pass this information onto the relevant people.

## Roles and Responsibilities

The responsibility of managing online safety can be demanding and challenging, and must therefore be appointed at managerial/committee level to personnel who are available when we are operational. (This will normally be the same person who will lead on child protection and safeguarding).

Lead Name: **Karen Double**

Contact details: 07761397535 or [karen@leapssuffolk.org.uk](mailto:karen@leapssuffolk.org.uk)

Deputy leads: Jenna Burton and Katie Finch

Email: [jenna@leapssuffolk.org.uk](mailto:jenna@leapssuffolk.org.uk) or [katie@leapssuffolk.org.uk](mailto:katie@leapssuffolk.org.uk)

Contact details: 07502 775685 or during each session

LEAPS Suffolk, Brightspace, 160 Hadleigh Road Ipswich IP2 0HH

## **OUR ONLINE 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, send messages 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 lead or deputy person for E-Safety immediately.
5. Be clear that I cannot maintain confidentiality if there is a concern about the welfare of an attendee.

### **WHAT ARE THE RISKS?**

There are many potential risks for children 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 online.
- Using a webcam in a closed area, away from other people.
- Accessing the web or using a mobile or PDA (Personal Data Assistant) 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/children or young person/people on the internet or by text messaging.
- Has links to children 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.

### **WHAT DO I DO IF I AM CONCERNED?**

If you have any concerns speak to the lead or deputy immediately. An online safety concern is a safeguarding concern

### **CONTACTS FOR REFERRING**

If the concern is about:

- A child/adult 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.suffolkscb.org.uk](http://www.suffolkscb.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.gov.uk](http://www.ceop.gov.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](http://www.iwf.org.uk)

**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.**

**MINIMISING THE RISKS:**

We will:

- Talk to attendees about what they are accessing on line.
- 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 attendees 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 attendees 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 attendees 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.
- Ensure all staff and volunteers have online safety training.
- Not give attendees access to any gaming opportunities, or mobile phones etc
- Limit when attendees use their phone during an Out, Not In! activity and regularly check in what they are doing.

**CCTV**

There is CCTV on the premises. The system is owned by Stone Lodge Academy and maintained by SOS who are appointed by Suffolk County Council.

LEAPS Suffolk do not have access to any images from the CCTV system.