Title	E Safety Policy
Linked Documents	Anti-Bullying & Harassment Policy Behaviour Policy Confidentiality Policy Data Protection Policy E-Safety Policy Handheld Device Policy Safeguarding Adults Policy Safeguarding Children and Young People Policy Social Media Policy Young People's Code of Conduct External Documents: Essex Safeguarding Children Board e-safety information for young people CEOP website
Contents	1: Introduction 2: Promoting E-Safety 3: Responding to E-Safety Concerns 4: Roles and Responsibilities

1. Introduction

This policy sets out how we promote e-safety, reduce risks related to online activity, and responds effectively to concerns. InterAct recognises that children and young people use digital technology in many aspects of their lives. While it offers huge opportunities for learning, connection, and creativity, it also carries risks. We are committed to ensuring our staff, volunteers, trustees, and beneficiaries are supported to use technology safely and responsibly.

Scope

This policy applies to all children, young people, and families engaging with the charity as well as all staff, volunteers, agents and trustees. The policy covers any use of digital technology, including websites, email, social media, messaging apps, and online platforms used for youth work through the use of a variety of devices including phones and games consoles.

Principles

We recognise that:

- **Safeguarding first:** the welfare of the children, young people and vulnerable adults who come into contact with our services is paramount and should govern our approach to the use and management of electronic communications. All children, regardless of age, disability, gender, racial heritage, religious belief, sexual orientation or identity, have the right to equal protection from all types of harm or abuse
- **Education and empowerment:** working in partnership with children, young people, vulnerable adults, their parents, carers and other agencies is essential in promoting their welfare and in helping them to be responsible in their approach to e-safety. The use of information technology (IT) is an essential part of all our lives; it is involved in how we as an organisation gather and store information, as well as how we communicate. It is also an intrinsic part of the experience of our children and young people, and is greatly beneficial to all.
- **Prevention and early intervention:** IT can present challenges in terms of how we use it responsibly and, if misused either by an adult or a young person, can be actually or potentially harmful to them. Risks should be minimised through proactive steps.
- **Transparency and accountability:** Concerns will be dealt with fairly, consistently, and in line with safeguarding procedures.

2. **InterAct will promote e-safety by:**

- appointing our Designated Safeguarding Lead as our E-Safety Coordinator
- encouraging responsible use of technology and model positive digital behaviour
- use our procedures to deal firmly, fairly and decisively with any examples of inappropriate IT use, complaints or allegations, whether by an adult or by a child/young person
- informing parents and carers of incidents of concern as appropriate
- reviewing and updating the security of our information systems regularly
- providing adequate physical security for InterAct IT equipment
- using secure and approved online platforms for charity activities
- ensuring that user names, logins and passwords are used effectively
- ensuring images of children, young people, vulnerable adults and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given
- any social media tools used in the course of our work with children, young people, vulnerable adults and families must be risk assessed in advance by the member of staff wishing to use them, and agreed by InterAct management
- providing effective management for staff and volunteers on IT issues, through supervision, support and training
- examining and risk assessing any emerging new technologies before they are used within the organisation
- promoting awareness of current e-safety issues (such as cyberbullying, grooming, scams, harmful content, and screen-time risks) when appropriate
- applying appropriate privacy and security settings on social media and online tools
- ensuring staff and volunteers understand safe online communication with young people, including boundaries and use of professional accounts
- prohibiting one-to-one unsupervised online contact between staff/volunteers and young people outside agreed platforms and times
- providing updates to trustees, staff, volunteers, and beneficiaries as new risks emerge
- maintaining clear reporting procedures for young people, staff, and parents to raise concerns

3. **Responding to and Reporting e-Safety Concerns**

Should any e-safety concern come to the attention of a member of staff or volunteer, or be reported to them, they should ensure that:

- all e-safety concerns are treated as safeguarding issues and respond in line with the Safeguarding Policy.
- we will respond proportionately and supportively, balancing the welfare of the child/young person with the need to protect others.
- we will involve parents/carers where appropriate, unless doing so places a young person at risk of harm.
- serious concerns (e.g. grooming, sexual exploitation, illegal content, significant cyberbullying) are reported to statutory agencies such as the police or children's social care
- any inappropriate, unsafe or unlawful IT activity ceases immediately
- that any children, young people, vulnerable adults or others are separated or encouraged to cease contact with any continuing risks, individuals or activities linked to the e-safety concern
- where possible, that any evidence of the e-safety concern is noted, to assist in any further investigation. This may include mobile phone messages, images, emails, website URLs, contact details, plus any comments or other information from those involved. However, they should be mindful that any further transmission of sexual images of children is also illegal

- e-safety concerns should be reported immediately to the appropriate lead worker, manager or E-Safety Coordinator, who will consider how the matter should be addressed
- InterAct's response to the e-safety concern may subsequently include contacting parents, the police, social services or other agencies (e.g., schools or colleges), in line with InterAct's Safeguarding Procedures, and to enable an effective multi-agency response, if required

4. Roles and Responsibilities

- **Trustees:** Oversee policy implementation and review
- **Designated Safeguarding Lead (DSL):** Lead on e-safety concerns, keep up to date with guidance, and ensure staff training
- **Staff and Volunteers:** Promote safe online behaviour, report concerns, and follow procedures
- **Young People:** Engage responsibly online and speak up if they feel unsafe
- **Parents/Carers:** Support their child's use of technology and work with the charity to promote safety