



## **InterAct e-Safety Policy**

This policy and the procedures that it underpins apply to all staff, including senior managers and the board of trustees, paid staff, volunteers and sessional workers, agency staff, students and anyone working on behalf of InterAct:

- to protect children, young people and vulnerable adults who participate in InterAct's services and who make use of information technology (such as mobile phones, games consoles and the Internet) as part of their involvement with us
- to provide staff and volunteers with the overarching principles that guide our approach to e-safety;
- to ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use information technology.

### **We recognise that:**

- 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 technologies;
- 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;
- 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 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 with each other. It is also an intrinsic part of the experience of our children and young people, and is greatly beneficial to all. However, 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.

### **InterAct will seek to promote e-safety by:**

- appointing a named e-safety coordinator
- developing a range of procedures that provide clear and specific directions to staff and volunteers on the appropriate use of ICT;
- supporting and encouraging the young people using our service to use the opportunities offered by mobile phone technology and the internet in a way that keeps themselves safe and shows respect for others;

- supporting and encouraging parents and carers to do what they can to keep their children safe online and when using their mobile phones and game consoles;
- incorporating statements about safe and appropriate ICT use into the codes of conduct both for staff and volunteers and for children and young people;
- use our procedures to deal firmly, fairly and decisively with any examples of inappropriate ICT use, complaints or allegations, whether by an adult or by a child/young person (these may include breaches of filtering, illegal use, cyberbullying, or use of ICT to groom a child or to perpetrate abuse);
- 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 ICT equipment;
- ensuring that user names, logins and passwords are used effectively;
- using only official email accounts provided via the organisation, and monitoring these as necessary;
- ensuring that the personal information of staff, volunteers and service users (including service users' names) are not published on our website;
- ensuring that 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 at an appropriate level
- providing effective management for staff and volunteers on ICT issues, through supervision, support and training;
- examining and risk assessing any emerging new technologies\* before they are used within the organisation.

[\* e.g. Specific guidance for the use of 'Zoom' video conferencing sessions for online meetings/sessions was written & implemented when sessions commenced in 2020]

## **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:

- any inappropriate, unsafe or unlawful activity ceases immediately, whether via the internet, mobile phone or other use of ICT
- 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/preserved, to assist in any further investigation, should that be necessary. 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/or disciplinary procedures, and to enable an effective multi-agency response, should that be needed.

### **Further guidance and information on e-safety, for young people**

The Essex Safeguarding Children Board have further information on e-safety for young people available at:

<https://www.escb.co.uk/young-people/staying-safe-online/>

You can also visit the CEOP website: <http://ceop.police.uk/>

### **Acknowledgement**

This policy (excluding the section on Responding to and Reporting e-Safety Concerns) was developed originally from an example policy on the Safe Network website, which has since been closed down.

In developing their example policy, Safe Network were indebted to Kent County Council for their work in this area. Many of the statements in the example have been taken or adapted from their *Schools and Settings e-Safety Policy Template 2012*.

+++++

InterAct's e-Safety Coordinator is Lesley Bailey: 01245-392053

Email: [lesley.bailey@interact.org.uk](mailto:lesley.bailey@interact.org.uk)