Subject	E Safety & Cyberbullying Policy
Document Reference	SAFE 01.09.05
Issue Number	9
Date	01/08/2024
Review	01/08/2026

Policy Statement

The purpose of this policy is to help ensure the safety and mental wellbeing of clients, Staff, Trustees, Volunteers and Beneficiaries when using virtual call centre platform, internet, social media platforms, and mobile devices. We recognise that E-Safety is not simply about such things as virus protection, internet filtering or other IT concerns. E-Safety and Cyberbullying are also about ensuring that technology is used in a manner that is safe and respectful of others.

Aims

Our aims are to **Educate,** to **Protect and** to **Support.** We will do this by:

- Ensuring necessary training for Life staff and volunteers is available in accordance with job roles.
- Ensuring all Life owned computers, laptops and mobile phones are virus and password protected in line with Life's IT Security policies.
- Ensuring where possible we educate on the dangers associated with the Internet and Online activities such as social media platforms.
- Protect all Life Staff and Volunteers from unacceptable behaviour from clients or other individuals when conversing via online pathways e.g email, text, telephone.
- Protecting as much as possible individual(s') personal safety, mental wellbeing and financial wellbeing when interacting with or on behalf of Life
- Ensuring that images of children and young people are used only after the purpose of their use has been explained and theirs, or a parent/guardian's written permission has been obtained.
- Supporting and referring to specialised help any client, staff, trustee, volunteer or beneficiary who has been affected by offensive materials or cyberbullying

Definitions

E-Safety

E-Safety is the term used to define the safe and responsible use of technology. This includes the use of the Internet and communication using electronic media such as emails and messaging services. Other recognised names for E-Safety are Internet Safety, Online Safety or Web Safety.

An E-Safety incident is considered to have occurred when an activity which uses Information Communication Technologies (ICT) endangers the personal safety, mental wellbeing or financial wellbeing of an individual.

Activities which are considered E-Safety incidents include but are not limited to:

- Accessing, viewing, copying or downloading illegal content or materials that are offensive
- Child pornography
- Sexting, sexual abuse or exploitation
- Abusive, threating language and behaviours
- Materials inciting racial hatred
- Derogatory language or remarks in relation to another person's culture, race, faith, gender or sexual orientation
- Violent materials that are seen to be connected to radicalisation
- Accessing sites that will place individuals at risk of radicalisation
- Committing fraud or identity theft
- Any other incident where it can be reasonably considered that the personal safety or wellbeing of an individual has been endangered by ICT.

Cyber Bullying

Is defined by the National Bullying Helpline as:

- Bullying online and any form of anti-social behaviour over the internet or via a mobile device. It is an attack or abuse, using technology, which is intended to cause another person harm, distress or personal loss.

Cyberbullying can happen over a wide range of social networking sites and websites may be targeted and concentrated on one person or a group. The tool used to enable Cyberbullying may be a computer or laptop, a mobile phone, a camera or recording device, a tablet or games-console or simply email or mobile text messaging. Some examples of cyberbullying can include:

- Spreading malicious and abusive rumours and gossiping
- Email or texting with threatening or intimidating remarks
- Mobbing – term used for a group or gang that targets a victim
- Repeated harassment
- Intimidation and blackmail
- Online stalking leading to harassment
- Posting embarrassing or humiliating images or videos without consent.
- Posting private details online without consent

- General bullying or stalking
- Grooming – enticing or goading a victim on-line to self-harm or commit a crime
- Setting up a false profile, Identity fraud or Identity theft
- Using gaming sites to attack or bully
- Theft, Fraud or deception over the internet

All of the above are recognised by the Police and Government laws under the term eCrime ,and are guided under the following legislation:

- The Protection from Harassment Act
- The Malicious Communications Act 1988
- The Malicious Communications (Northern Ireland) Order 1988
- The Communications Act 2003
- Obscene Publications Act 1959
- Computer Misuse Act 1990
- Cyberbullying in the Workplace.

Client and Counsellor consideration will also be guided by BACP Code of Ethics and BACP Online and phone therapy (OPT) Competence Framework.

Procedure

All E-Safety incidents or suspected incidents must be reported to your area Safeguarding Department Representative (SDR) or other suitable manager. Any Life IT equipment or mobile phones should be kept secure and where necessary the Systems and IT Manager contacted immediately to secure relevant evidence such as IP addresses. Other evidence such as screen shots should be secured at time of incident or preserved as soon as possible.

Reporting procedure should follow the following steps:

- Inform your area SDR or a member of the Safeguarding Committee. They will open a Safeguarding Folder and reporting on the concern will be guided by them
- SDR will report to police and any other needed agencies and will be guided by their advice and instructions
- Monitoring and support will be given to the victim(s), staff and volunteer(s) throughout the safeguarding journey where necessary

Life – Trauma Informed promise

By submitting this Policy the author is confirming that they have considered the six principles of a Trauma Informed approach as a means for reducing the negative impact of trauma experiences and supporting mental and physical health outcomes. This includes putting people before protocol, creating a culture of thoughtfulness and

communication, and continuously doing our best to learn about and adapt to the different and changing needs of the individuals we work with.

Life– GDPR compliance

o This policy does not concern the collection, storage, or processing of any personal data, nor does it affect any other policies or systems that concern personal data.

(If you have highlighted the above there is no need to complete the rest of this declaration)

1. I have read and understood the Life GDPR Policy and confirm that the Policy above fully complies with it in all areas.
2.

	Lawful Basis for this Policy:	Add 'yes' to which one(s) apply
a	Consent	√
b	Contract	
c	Legal Obligation	√
d	Vital interests	√
e	Public Tasks	
f	Legitimate Interests	
g	Special Category (e.g., Children's data)	√
	Please state the purpose for special category:	Using child(rens) images with adult in charge consent.

3.

	I confirm that all personal data is:	Add 'yes' to which one(s) apply
a	Held only in the locations detailed in this Policy	Yes
b	Used only for the purposes stated	Yes
c	Held securely	Yes

4.

	By signing this Policy, you are agreeing to the following:
a.	A Data Processor Agreement is in place with all external organisations (Data Processors) who are in receipt of personal data under the terms of this Policy
b.	The relevant Policy Notices under this Policy have been published in an appropriate manner.

5.

	The person(s) responsible for data protection covered by this Policy are: (List Persons below)	Insert Date
	Liz Lloyd	01/08/2024

6. As the above-named person, I confirm that this Policy complies with the Data Protection Act 2018

Signed Liz Lloyd Name: Liz Lloyd Date: 01/08/2024

Note: Life has chosen not to appoint a Data Protection Officer which is permitted under GDPR and so this responsibility is devolved to the appropriate person named under this Policy.