



General Manual

Subject: ESafety & Cyberbullying Policy

Document Number: 1.09.5

Issue 5

Date: 01 June 2020

Review: 01 June 2021

Purpose

To help ensure the safety and mental wellbeing of clients, Staff, Trustees, Volunteers and Beneficiaries when using the internet, social media or mobile devices. We recognise that ESafety is not simply about such things as virus protection, internet filtering or other IT concerns. ESafety is 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
- Ensuring where possible we educate on the dangers associated with the Internet and Online activities such as social media platforms.
- 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 /guardians 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

ESafety

ESafety is the term used to define the safe and responsible use of technology. This includes the use of the Internet and other means of communication using electronic media such as emails and messaging services. Other recognised names for ESafety are 'internet safety' 'Online Safety' or 'Web safety'.

An ESafety incident is considered to have occurred when an individual is the victim of an activity which uses Information and Communication Technologies (ICT) to endanger the personal safety, mental wellbeing or financial wellbeing of another individual.

Activities which are considered ESafety 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
- Materials inciting racial hatred
- Violence 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:

Cyberbullying is 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 such as Facebook, Twitter and other interactive forums. It 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
- On-line stalking leading to harassment
- Posting embarrassing or humiliating images or videos without consent.
- Posting private details on-line 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 others under the term eCrime.

Safeguarding and Reporting Procedure

All ESafety incidents or suspected incidents must be reported to your area **Safeguarding Department Representative (SDR)** or other suitable manager. Any Life IT equipment or mobile phone should be

kept secure and where necessary the Communications and IT Department contacted immediately to secure relevant evidence. Other evidence such as screen shots should be secured.

Reporting procedure should follow the following steps:

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

Legislation

Protection from Harassment Act <http://www.legislation.gov.uk/ukpga/1997/40/contents>

Computer Misuse Act 1990 - <http://www.legislation.gov.uk/ukpga/1990/18/contents>

Data Protection Act 1998- <http://www.legislation.gov.uk/ukpga/1998/29/contents>

Malicious Communication Act 1998- <http://www.legislation.gov.uk/ukpga/1988/27/contents>

The Communications Act 2003 <http://www.legislation.gov.uk/ukpga/2003/21/contents>

Obscene Publications Act 1959

http://www.legislation.gov.uk/ukpga/1959/66/pdfs/ukpga_19590066_en.pdf

Cyberbullying in the Workplace <https://archive.acas.org.uk/index.aspx?articleid=5992>

Working together to Safeguard children / young people (2015)

<https://www.gov.uk/government/publications/working-together-to-safeguard-children--2>

Prevent duty's statutory Guidance regarding Online Safety and Radicalisation – UK Home Office 2019

<https://www.gov.uk/government/publications/prevent-duty-guidance>

Resources

The National Bullying Helpline <https://www.nationalbullyinghelpline.co.uk/>

NSPCC <https://www.nspcc.org.uk/what-is-child-abuse/types-of-abuse/bullying-and-cyberbullying/>

Life polices - GDPR compliance

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 (tick which one(s) apply)
 - a. Legal obligation ☐
 - b. Legitimate Interest ☒
 - c. Contract ☐
 - d. Vital Interest ☐
 - e. Consent ☐

- f. Special Category (e.g. Children's data) ☐

Please state the purpose for special category _____

3. I confirm that all personal data is:

- a. held only in the locations detailed in this Policy ☐
b. used only for the purposes stated ☐
c. held securely ☐

4. 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:

(tick to confirm) ☐

5. The relevant Privacy Notices under this Policy have been published in an appropriate manner:

(tick to confirm) ☐

6. The person(s) responsible* for data protection covered by this policy are:

_____ Liz Lloyd _____ (date) __1st July 2020_____
_____ (date) _____

7. As the above named person I confirm that this Policy complies with the General Data Protection Regulations 2018

Signed _____ Liz Lloyd _____

Name _____ Liz Lloyd _____

Date _____ 1st July 2020 _____

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.