Life Beacon

INFORMATION GOVERNANCE

2025

www.LifeBeacon.org

Table of Contents

1.0 Introduction

- Information is a valuable asset and fundamental to all the activities across and within Life Beacon International's(LBI) departments.

- Information as captured here is defined as any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphical, narrative, or audio-visual.

- The governance of information across and within LBI's departments is to ensure a secure, effective, efficient, and confidential use of data. This is a mandatory practice for all trustees, coordinators, volunteers and other stakeholders.

1.1 Principles

1.1.1 Directness and Quality assurance

1.1.1.1 Trustees, coordinators, volunteers and other stakeholders, have the right to know how their data is used and it is LBI's responsibility to assure the accuracy and security of the data held.

1.1.1.2 LBI's non-confidential information are made available through the website and social media accounts and can also be sought under the Freedom of Information Act.

1.1.1.3 LBI has procedures and arrangements for handling queries about data openness and quality from trustees, co-ordinators, volunteers and other stakeholders.

1.1.2 Information management and security

1.1.2.1 LBI adheres to International Organisation for Standardisation (ISO) standards for data management, procedures and working practices to ensure the secure management of its information assets.

1.1.2.2 Risk assessment and audits are carried out regularly to mitigate significant risks and reduce the exposure to potential security threats to information.

1.1.2.3 Coordinators and volunteers of LBI are trained to manage information responsibly, effectively, and securely. Co-ordinators and volunteers have a responsibility to understand and apply policies for handling information.

1.1.2.4 All incidents regarding information vulnerabilities are monitored and controlled under LBI's instance reporting system to mitigate the actual and potential breaches in privacy, confidentiality, and security.

1.1.2.5 Co-ordinators and volunteers are given the necessary access to the LBI's MS Teams portal and One Drive- the main platforms for information storage.

2.0 Sub-policies

2.1 Information Creation Policy

2.1.1. All information created is either classified as 'not sensitive', 'confidential' or 'highly confidential.

2.1.2 LBI has arrangements and systems in place to create, monitor and protect information from all known threats whilst assuring quality.

2.2 Information Storage Policy

2.2.1 All stored information should comply with all legal and regulatory requirements relating to the retention of information including long term preservation (physical and digital).

2.2.2 All files should not be stores locally on personal computers.

2.2.3 All original files should be deleted from personal computers as soon as possible.

2.3 Information Sharing policy

2.3.1 Information is to be shared securely and safely within and across LBI's departments, outlining tools that can assist in the sharing of information.

2.3.2 Information classified as 'not sensitive' can be shared openly amongst associates, and volunteers via LBI's MS Teams or OneDrive only.

2.3.3 'Confidential' information may be shared internally or externally in a restricted and secured manner- mainly via LBI's Teams portal or OneDrive only and with approval from the data owner.

2.3.4 'Highly confidential' information requires approval from the chairperson before being shared such as, donor, beneficiary, human resource and financial information.

2.3.5 LBI will ensure that Intellectual Property (IP) is managed in a manner that meets all legal and contractual obligations and requirements.

2.4 Information Security Policy

2.4.1 Information Security as captured here is the management of information to ensure adequate access and use whilst simultaneously preventing unauthorized access. It includes processes to reduce the risk of unauthorised copying, modification, or deletion of information.

2.4.2 LBI has suitable arrangements for the monitoring of activities across information systems to prevent or detect actual or potential security breaches and take appropriate action in response.

2.4.3 LBI will undertake regular data security audits and promote confidentiality and security practices to all its stakeholders through its routine training.

3.0 Responsibilities

3.1 Trustees and Coordinators

3.1.1 To approve LBI's Information Governance policy.

2.1.2 To ensure that LBI's Information Governance policy is adhered to in any dealings with third party individuals and organisations.

3.1 All volunteers and coordinators

3.2.1 To promote an effective information management culture, including information security, through the continued delivery of awareness and training.

3.2.2 To treat personal information lawfully and correctly,in particular, adhering to the Key Principles of Data Protection, contained in the Data Protection Act 2018.

3.2.3 To ensure information assets are effectively controlled, leveraged, and optimised for the benefit of LBI.

3.2.4 To adhere to the risk-based approach of information management across its lifecycle whilst adhering to quality and value-added requirements.

3.2.5 To ensure attention to security, protection, quality, usability, retrievability and preservation are given across the information lifecycle.

3.2.6 Familiarise yourself thoroughly with your device and its security features to identify any potential security threats.

3.2.7 To ensure that separate accounts are used on devices shared with family members.

3.2.8 To ensure that all relevant security and anti-virus features are enabled, where appropriate.

3.2.9 To set appropriate passwords, passcodes, passkeys or biometric equivalents.

3.2.10 To ensure that sections of Confidential and Highly Confidential Information are not retained on personal devices.

3.2.11 To report any suspicious activities to the Chairperson or the Information Manager.

4.0 Key external Links

Data Protection Act 2018: https://www.gov.uk/data-protection

Freedom of Information (FOI) Request: https://www.gov.uk/make-a-freedom-of-information-request

How copyright protects your work: https://www.gov.uk/copyright