Lifeworks Charity Limited

General Data Protection Policy

(UK GDPR)

June 2022

Author: Head of Finance & Governance

Reader Information

Title	Data Protection Policy V5
Document purpose/summary	The purpose of this policy is to assist employees by providing clear guidance about Data Protection.
Author	Head of Finance & Governance
Ratification date	[06/2022]
Review date and frequency	Annually
Target audience	All Lifeworks staff
Circulation	Electronic: Employee Portal Written: Upon request to HR Please contact HR f you require this document in an alternative format.
Consultation process	SLT
Equality analysis checklist completed	Yes
References/sources of information	Information Commissioners Office www.ico.gov.uk Social Care Assessment Data Protection Tool Kit Digital Social Care
Associated documentation/cross referenced policies	Confidentiality and Information Sharing Policy Data Retention and Destruction Policy IT Security Policy Acceptable use of Mobile Phone Policy Publicity Social Media and Photos Privacy Policy for those who use our services General Privacy Policy Data Subject Access Request
Supersedes document	Data Protection V4

Version Control

Version no.	Type of change	Date	Originator of change	Description of change
V2	Update	September 2020	Jo Parsons	Minor
V3	Regulatory update	May 2018	Jo Parsons	To comply with GDPR
V4	Regulatory update	July 2021	Jo Parsons	Regulatory change following Brexit. To meet requirements of Social Care Data Protection Tool Kit for Impact assessments and Spot Checks
V5	Complete review	June 2022	Jo Parsons	Section re-writes

1 Introduction

1.1 Lifeworks is committed to all aspects of data protection and take seriously its duties, and the duties of its employees under the General Data Protection UK Regulation (UK GDPR). We will be open and transparent with those who use our services and those who lawfully act on their behalf in relation to their education, care and treatment. We will adhere to our duty of candour responsibilities as outlined in the Health and Social Care Act 2012.

2 Purpose

2.1 The purpose of the Data Protection Policy is to:

2.1.1 Support the 10 Data Security Standards, the General Data Protection Regulation (2016), the Data Protection Act (2018), the common law duty of confidentiality and all other relevant national legislation.

2.1.2 Assist the Board of Trustees, Staff, Volunteers, contractors and any other people working on behalf of Lifeworks of their responsibilities in respect of UK GDPR when gathering, using, sharing personal data about individuals, these include Service Users, Beneficiaries, Employees, Volunteers, Donors, Customers and Suppliers.

3 Scope

3.1 This policy applies to all personal data processed by Lifeworks, either in hard copy or digital copy, this includes special category data.

3.2 The policy applies to all staff, including temporary staff, agency staff and contractors.

3.3 This policy shall be reviewed at least annually.

3.4 Lifeworks is registered with the Information Commissioner's Office as an organisation that processes personal data.

4 Responsibilities

4.1 The Board of Trustees is ultimately responsible for the content of the Data Protection Policy, its implementation and review.

4.2 Data Controller

The key responsibilities are:

4.2.1. Provide support and advice to managers and employees on the operation of the policy and guidelines, where necessary.

4.2.2 Overseeing changes to systems and processes;

4.2.2. Monitoring compliance with the GDPR and the Data Protection Act 2018;

4.2.3. Completing DPIA;

4.2.4. Reporting on data protection and compliance with legislation to the Board of Trustees.

4.2.5. Liaising, if required, with the Information Commissioner's Office (ICO).

4.3 Employee responsibility

4.3.1 To familiarise themselves with the UK GDPR Policy and other associated policies and guidelines.

4.3.2 To participate in appropriate training relating to UK GDPR

4.4 Managers responsibility

4.4.1 To familiarise themselves with the UK GDPR Policy and other associated policies and guidelines.

4.4.2 Ensure staff are aware of the UK GDPR Policy and other associated policies and guidelines.

4.4.3 Ensure all data protection breaches, complaints/allegations are reported to the Data Controller.

4.4.4 To participate in appropriate training relating to UK GDPR

5 Data Protection Principles

5.1 Lifeworks is committed to processing data in accordance with its responsibilities under UK GDPR. Article 5 of the GDPR requires that data shall be:

5.11 Processed lawfully, fairly and in a transparent manner in relation to individuals.

5.12 Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest or statistical purposes shall not be considered to be incompatible with the initial purposes.

5.13 Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

5.14 Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay.

5.15 Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

5.16 Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

6 Lawful, fair and transparent processing

6.1 To ensure its processing of data is lawful, fair and transparent, Lifeworks shall maintain a Register of Systems.

6.2 The Register of Systems shall be reviewed at least annually.

6.3 Individuals have the right to access their personal data and any such requests made to Lifeworks shall be dealt with in a timely manner, without undue delay and at the latest within one month of receipt. Requests should be made using the guidance available in the Subject access request guidance procedure.

7 Purpose Limitation

7.1 We will establish and maintain policies to ensure compliance with the Data Protection Act 2018, Human Rights Act 1998, the common law duty of confidentiality, the General Data Protection Regulation and all other relevant legislation.

7.2 We will establish and maintain associated policies for the controlled and appropriate sharing information with other agencies, taking account all relevant legislation and citizen consent.

7.3. Where consent is required for the processing of personal data we will ensure that informed and explicit consent will be obtained and documented in clear, accessible language and in an appropriate format. The individual can withdraw consent at any time through processes which have been explained to them and which are outlined in our Record Keeping Policy: Withdrawal of Consent procedures. We ensure that it is as easy to withdraw as to give consent.

8 Data minimisation

8.1 Lifeworks will ensure that personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

9 Accuracy

9.1 Lifeworks will take reasonable steps to ensure personal data is accurate.

9.2 Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that data is kept up to date.

10 Storage limitation

10.1 To ensure that personal data is kept no longer than is necessary, Lifeworks has a Retentions & Destruction Policy including a retentions schedule for each area in which personal data is processed and review this process annually.

10.2 The Retentions Policy shall consider what data should/must be retained, for how long, and why.

11 Data protection by design & by default

11.1 We shall implement appropriate organisational and technical measures to uphold the principles outlined above. We will integrate necessary safeguards to any data processing to meet regulatory

requirements and to protect individual's data rights. This implementation will consider the nature, scope, purpose and context of any processing and the risks to the rights and freedoms of individuals caused by the processing. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/.

11.2. We shall uphold the principles of data protection by design and by default from the beginning of any data processing and during the planning and implementation of any new data process.

11.3. Prior to starting any new data processing, we will assess whether we should complete a Data Protection Impact Assessment (DPIA) using the ICO's screening checklist:

11.4. All new systems used for data processing will have data protection built in from the beginning of the system change.

11.5. All existing data processing has been recorded on our Record of Processing Activities. Each process has been risk assessed and is reviewed annually.

11.6. We ensure that, by default, personal data is only processed when necessary for specific purposes and that individuals are therefore protected against privacy risks.

11.7. In all processing of personal data, we use the least amount of identifiable data necessary to complete the work it is required for and we only keep the information for as long as it is required for the purposes of processing or any other legal requirement to retain it.

11.8. Where possible, we will use pseudonymised data to protect the privacy and confidentiality of our staff and those we support.

12 Breach

12.1 **Assessing the risk** - in the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, Lifeworks will promptly assess any risks associated with the breach. In particular, we will assess the potential adverse consequences for individuals; how serious or substantial these are; and how likely they are to happen.

12.2 **Notification -** we will be clear about who needs to be notified and why.

12.2.1 Lifeworks will as a matter of course immediately notify purchasers if there are any security incidents.

12.2.2 The GDPR introduces a duty on all organisations to report certain types of personal data breach to the ICO. You must do this within 72 hours of becoming aware of the breach, even if all of the information is not yet available. To report a breach please follow the following link. https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/

12.2.3 If a breach is likely to result in a high risk to the rights and freedoms of individuals, Lifeworks staff must inform those concerned directly and without undue delay. In other words, this will take place as soon as possible (prior to informing the ICO) to help mitigate immediate risk of damage and to help individuals take steps to protect themselves from the effects of the breach.

12.2.4 Other regulatory bodies such as OFSTED, CQC, and the police.

12.3 **Containment and recovery** – the response to the incident should include a recovery plan and, where necessary, procedures for damage limitation.

12.4 **Evaluation and response** – any breach will be investigated to establish the cause and also to evaluate the effectiveness of our response.

NOTIFICATION CONTACTS

Notification for Devon County Council is via KeepDevonSafe@devon.gov.uk

ICO – Data breach reporting form https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/

ICO Call for advice Monday to Friday between 9am and 5pm - **0303 123 1113**