

Kisimul

DP02 | Data Protection

Policy and Procedure

Document Information

Document:	DP02 Data Protection Policy and Procedure
Division:	Data Protection & Information Systems
Document owner position:	Data Protection Officer
Authorising committee:	Information Governance Committee
Date authorised:	April 2025

Document Publication & Review

Date first published:	April 2019
Date of last revision:	April 2025
Date of next review:	April 2027
This document will be reviewed at least every 2 years, or sooner if legislation/guidance changes	
A full Change Log can be found at the back of this document	

Equality, Diversity & Inclusion Statement

No person or group should suffer oppression or lack of opportunity because of a protected characteristic. Kisimul Group opposes all forms of unlawful discrimination, and we are committed to encouraging equality, diversity, fairness and inclusion in the application of our policies so that everyone has equal access and feels welcome and at ease. To achieve this aim, the application and accessibility of our policies, and the decisions and outcomes arising from our policies, may be monitored to ensure their use is fair, equal and consistent irrespective of any characteristic as may be defined by the Equality Act 2010. This is to ensure that we are listening to people and appropriately understanding their needs, and are tailoring the way we interact and publish or act on our policies to ensure we are promoting equal access and opportunity at all times.

Contents

Contents	3
1. Introduction	3
2. Scope.....	3
3. Definitions	4
4. General provisions and responsibilities	5
5. Legislation overview	5
6. Individuals' rights	6
7. Compliance with the principles of data protection	6
8. Complaints	7
9. Monitoring compliance	7
10. Training requirements	8
Appendix 1 – Retention Schedule	8
Appendix 2 – DPO Poster	8

1. Introduction

As Kisimul, we need to gather and use certain personal data and information about those who take or use services from us, do business with us, as well as our employees, trustees and volunteers or independent contractors. We recognise that the lawful and correct handling of all personal information is extremely important to maintain a level of confidence. This policy describes how we will comply the requirements and obligations set out in the *Data Protection Act 2018 (DPA)* and the *UK General Data Protection Regulation* and *EU General Data Protection Regulation* (collectively referred to as *GDPR*) where the EU is applicable to our service users, patients, or their families.

2. Scope

This policy applies to all Kisimul colleagues, including bank and agency colleagues, as well as to the people we support and/or educate, any visitors or contractors, and anyone else whose data we collect and process in any way.

This policy applies to all personal data in all formats including manual or paper records, electronic records and systems, images and sound, emails and text messages, and information published in information leaflets or on our websites.

3. Definitions

3.1 Personal Data

Information about an identified or identifiable natural person (living individual) – someone who can be identified directly or indirectly including with the use of an online identifier.

3.2 Special Category Data (Sensitive Personal Data)

Personal data of an individual that relates to their racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health, sex life or orientation.

NB: The processing of data that is criminal data i.e. it relates to Offences or alleged offences, court proceedings or sentencing, fall within the EU Law Enforcement Directive and part 3 of the *DPA*.

3.3 Data Subject

The living individual who is the subject of the personal data, the natural person (we refer to them as individuals in our policies).

3.4 Controller

A natural or legal person, public authority, agency, or other body that determines the purposes and way in which personal data is processed. Kisimul Group Limited are the Controller.

3.5 Data Processor

A natural or legal person, public authority, agency, or other body that processes personal data on behalf of a Controller.

3.6 Processing

Any operation on the data including: obtaining/collecting, recording, organisation, storage or holding the personal data, disclosure; and any other operation on this e.g. destruction.

3.7 Responsible Person

This is someone appointed within the company to take responsibility for compliance with this policy and the legislation.

3.8 Data Protection Officer (DPO)

An employee or contracted person who has expert knowledge of data protection law and practices, and the ability to undertake the legislated tasks.

4. General provisions and responsibilities

4.1.1 All stages of the lifecycle of personal data are covered by this policy:

- Obtaining, gathering or collection of data.
- Storage and security of data and any information this data creates.
- Use and disclosure of data and any information this data creates.
- Sharing of data and any information this data creates.
- Disposal and destruction of data and any information this data creates.

4.1.2 As an organisation that provides health care and holds [special category data](#) in the form of health records, we are required to appoint a [Data Protection Officer](#). Their contact details are: Debra.Fullerton@kisimul.co.uk. They have an appropriate level of knowledge to provide advice on data protection matters and they will liaise with the ICO when required.

4.1.3 We will maintain our registration with the Information Commissioner's Office and the registration number is ZB007428.

4.1.4 We will also maintain our Data and Security Protection Toolkit Assessment and our company ODS code is A6V0.

4.1.5 Managers within Kisimul Group will be nominated to take responsibility for ongoing compliance with this policy.

4.1.6 All employees have a responsibility to read and comply with this policy.

5. Legislation overview

5.1.1 The *DPA 2018* and *GDPR* require all organisations that process personal data to follow certain rules (Principles). This legislation also defines certain terms and gives individuals a number of rights. There are six key Principles within *GDPR* that provide a framework for good practice and the proper handling of personal data. These are supported by a seventh principle of Accountability. We have summarised these here.

5.1.2 Personal data shall be:

- Processed lawfully, fairly and in a transparent manner ("lawfulness, fairness and transparency").
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ("purpose limitation").
- Adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed ("data minimisation").
- Accurate and, where necessary, kept up to date; every reasonable step to ensure inaccurate data are erased or rectified without undue delay ("accuracy")
- Kept in a form which permits identification of the individual for no longer than is necessary for the purpose which the data are processed ("storage limitations").
- 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 (“integrity and confidentiality”).

5.1.3 The additional principle of “Accountability” requires an organisation to be accountable for its actions, how it processes personal data and able to demonstrate compliance.

6. Individuals’ rights

6.1.1 We recognise and acknowledge that individuals have 8 Rights under GDPR, and we will ensure that these can be fully complied with:

- The right to be informed that we are processing their personal data (generally via a Privacy Notice).
- The right to access their own personal data (known as a “Subject Access Request” or “Data Subject Access Request”). Such requests are covered by ***DP03 Data Subject Access Requests and General Rights Requests Policy***.
- The right to rectification.
- The right to erasure (also known as the “Right to be forgotten”).
- The right to prevent restrict processing in certain circumstances.
- The right to data portability.
- The right to object to processing of personal data in certain circumstances.
- The right not to be subject to a decision based solely on automated processing including profiling.

6.1.2 Not all Rights are absolute, which means that some will have to meet certain requirements before they can be actioned. If we cannot action them, we will explain why.

6.1.3 More information about the individual’s rights can be found on the ICO website at www.ico.org.uk.

7. Compliance with the principles of data protection

To enable us to fully comply with the legislation, we will:

7.1.1 Inform individuals about our reasons for collecting and processing their personal data, including the legal basis for this.

7.1.2 Be clear on our correspondence about who we are, including use of signatures on emails and the use of an out-of-office message or auto-reply when this is appropriate.

7.1.3 Only collect and hold the data and information which are needed and follow all necessary conditions to enable us to do this, including obtaining consent where necessary.

7.1.4 Only use the data and information collected for the purpose specified or compatible purposes, and make individuals aware of any other use or sharing.

7.1.5 Only use the data and information for marketing of services where the individual has chosen (consented) to receive this or where we are allowed to do so by law.

7.1.6 Make every effort to ensure data and information are accurate and up-to-date, and where opinions or intentions are recorded, that these are professionally expressed.

7.1.7 If we use images or video, we will ensure that we have consent and we tell the individual about how we are going to use it (this applies to all individuals including colleagues – see ***DP08 Use of Data Subject Images Policy and Procedure***).

7.1.8 Follow our Retention Schedule (available at [Appendix 1](#)) when determining how long the data and information should be kept for.

7.1.9 Ensure that any transfers or sharing of data or information are undertaken with suitable safeguard measures and where necessary, suitable information sharing agreements are in place.

7.1.10 Ensure that we keep the data and information secure, preventing unauthorised access or processing or accidental loss.

7.1.11 Implement policies to ensure the proper and safe use of personal data including a clear desk (see ***DP07 Clear Desk and Screen Policy***), confidentiality (see ***HR13 Code of Conduct Policy and Procedure***) and policies that limit the use of mobile devices or removable media such as encrypted USB devices (see ***IT01 Information Systems Policy, IT02 Remote Working, Mobile Device and BYOD Policy*** and ***IT03 Portable Devices in the Workplace Policy***).

7.1.12 Ensure that any software used is current (up-to-date), all equipment used has sufficient technical measures in place such as anti-virus software, and all those who need access to our network or systems have unique logins and passwords (see ***IT04 Access Control Policy***).

8. Complaints

8.1.1 If an individual is unhappy with the way in which we have handled their personal data or information or is unhappy with our response to a Subject Access Request or any other of their rights, they can submit a complaint to us or directly to the ICO. We would like to encourage them to contact us in the first instance as we would like the opportunity to resolve the complaint.

8.1.2 These complaints will be passed to the Data Protection Officer (DPO) and will be investigated in line with the requirements of the legislation.

8.1.3 The individual does have the option of complaining to the ICO and can submit this using their online form at <https://ico.org.uk/make-a-complaint/>

9. Monitoring compliance

9.1.1 We will ensure that policies and procedures are in place to support our compliance. This will include maintaining details of processing, information assets and systems used, and the Retention Schedule at [Appendix 1](#).

9.1.2 Operational Managers and the Quality team will monitor compliance with this policy during audits, examination of data, site visits and Pulse tests.

9.1.3 The **Data Protection Officer** has responsibility to report serious non-compliance in information security to Kisimul Executive Board. Information security is a standard agenda item at the quarterly Information Governance Committee meeting.

9.1.4 In the event of a breach of the *DPA/GDPR* leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access to personal data will be investigated and dealt with in line with **DP04 Data Protection Breach Notification Policy and Procedure**. If a breach is found to meet the criteria for reporting to the ICO, this will be undertaken promptly and any recommendations or instructions received from the ICO as a result of their assessment or investigation will be implemented by us.

10. Training requirements

All employees will be provided with training and awareness in data protection and security to enable them to handle personal data correctly. Any independent contractors will be required to provide proof of equivalent training or complete the training provided by us.

Appendix 1 – Retention Schedule

The retention schedule is available to all Kisimul colleagues on SharePoint:

<https://kisimul.sharepoint.com/:b:/s/Policies/IQCS2NSVpWoaQIVKD4SToamTAbUtq1oH8V0JfOivTxjsKrl?e=DedTaD>

Appendix 2 – DPO Poster

The DPO poster is available to all Kisimul colleagues on SharePoint:

https://kisimul.sharepoint.com/:b:/s/Policies/IQBIKPOa4_ONSb2h9h9_Te_aAeeyvM-yT8EK5caBHLYQ4gM?e=snjX79

