Kisimul

Data Protection

Policy and Procedure

Document Information

Document:	DP02
Division:	Quality and Compliance
Document owner position:	Head of Risk and Governance
Authorising committee:	Performance and Effectiveness Committee (PESC)
Date authorised:	April 2023

Document Publication

Date document first published:	April 2019
Date of last revision:	April 2023
Date of next review:	April 2025

Authorised document change log recorded at the back of this document

This document will be reviewed at least every 2 years

Contents

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.

Scope

This policy applies to all directors, trustees, employees, and volunteers of Kisimul and any independent contractors working on our behalf.

For the purpose of this policy the term 'employee' will be used to refer to Kisimul employees, and all directors, trustees, and volunteers, and any independent contractors where applicable.

This Data Protection Policy will apply 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.

Definitions

We include the following to help with understanding of this policy and the legislation. This is not an exhaustive list of definitions or terms which can be found in the legislation or on the Information Commissioner's Office (ICO) website at www.ico.org.uk

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.

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.

Note: 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.

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).

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

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

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.

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

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.

General Provisions and responsibilities

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.

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.

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

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

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

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

The Chief Executive Officer has overall responsibility for ensuring compliance with national and local standards that are reflected in the organisations policies.

Legislation overview

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.

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 process ('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').

The additional principle of 'Accountability' requires all organisations to be accountable for its actions, how it processes personal data and being able to demonstrate compliance.

Individual's Rights

We recognise and acknowledge that individuals have 8 Rights under GDPR, and we will ensure that these can be fully complied with. The rights for individuals include:

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');

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.

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 the reason to individuals.

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

Compliance with the principles of data protection

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

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

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;

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;

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

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

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;

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 employees);

Follow our Retention Schedule when determining how long the data and information should be kept for;

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;

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

Implement policies to ensure the proper and safe use of personal data including a clear desk, confidentiality and policies that limit the use of mobile devices or removable media such as encrypted USB devices;

Ensure that any software used is current (up to date) and 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.

Complaints

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.

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

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/

Supporting this Policy

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.

We will ensure that our policies and procedures are in place to support our compliance. This will include maintaining details of processing, information assets and systems used, and a Retention Schedule.

Operational Managers and the Quality team will monitor compliance with this policy during audits, examination of data, site visits and Pulse tests. The DPO has responsibility to report serious none-compliance in information security to Kisimul Executive Board. Information security is a standard agenda item at the quarterly PESC meeting.

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 appropriately. 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.

More information

More information on data protection can be found on the Information Commissioner's website at www.ico.org.uk.

Reviews

We will review this policy on a bi-annual basis, or when legislation changes.

THE SCHEDULE

DATA PROCESSING ACTIVITIES

Type of data	Type of data subject	Type of processing	Purpose of processing	Type of recipient to whom personal data is transferred	Retention period	Lawful Basis for processing (s.5)
• Name • DOB • Address • Family details • Medical history • Education history • Details shared by previous provider in relation to any of the above.	Prospective Students / Residents.	The collection of details when considering whether a prospective Student/Resident will be placed with Kisimul Group.	To identify whether or not the data subject will benefit from a placement at Kisimul Group and to prepare a schedule of costs for the referring authority.	Employees and staff members, this may include administration staff, operation managers, assistant psychologists and finance teams.	6 months after the prospective student / resident application has been declined or has otherwise not been taken up.	Consent from a data subject (or via their legal guardian). In order to perform our obligations pursuant to contracts entered into with the Legal Guardian of a Student. Accordingly, we rely on "legitimate interest" and the legitimate interest is: carrying out a contract with the party by which the data subject will be a Student/Resident. To perform our obligations pursuant to contracts entered into with a health authority or agency. Accordingly, we rely on "legitimate interest" and the legitimate interest is: the provision of a health care and education at the request of local health authorities and agencies. Where we process special categories of data pursuant to such contracts, we do so on the basis that "processing is necessary for the purposes of provision of health or social care or treatment or the management of health or social care systems and services pursuant to contract with a health professional".

• Name • DOB • Address • Family details • Medical history • Education history • Details shared by previous provider in relation to any of the above. • CCTV footage • Photos and videos (as part of care/ education record)	Current Students / Residents.	Planning and reviewing care and education. Updating records as details change. Preparing reports including exit reports when Students / Residents leave. Passing information to a third party to safeguard an individual (e.g., to the police and local authorities - LSAB & LSCB). Conducting audits and internal inspections.	To ensure that Students / Residents are well cared for and well educated. To keep people safe. To comply with the requirements of the regulator – i.e. Ofsted and CQC. To review and record student/ resident development and/ or progress.	Employees (which may include support staff, education staff and management) and contractors such as therapists and consultants who are not employees. Finance staff can access some of the detail from perspective of managing accounts with local authorities in order to process invoices for payment. Compliance team can access details when carrying out audits / internal inspections. Local authorities and referring partners, carry out audits receive reports and exit information. Ofsted and CQC review details during statutory inspections.	For children: 75 years from the last date of entry. This is a required in order to comply with the Care Act the Mental Capacity Act and the Children's Home Regulations. For adults: 20 years from the last date of entry. CCTV footage is systematically deleted every five weeks, unless a request to view images (by, for example, the police) is received before the 5 week period has expired.	Consent from a data subject or their legal guardian. In order to perform our obligations pursuant to contracts entered into with the Legal Guardian of a Student/ Resident. Accordingly, we rely on "legitimate interest" and the legitimate interest is: carrying out a contract with the party by which the data subject will be a Student/ Resident. To perform our obligations pursuant to contracts entered into with a health authority or agency. Accordingly, we rely on "legitimate interest" and the legitimate interest is: the provision of a health care and education at the request of local health authorities and agencies. Where we process special categories of data pursuant to such contracts, we do so on the basis that "processing is necessary for the purposes of provision of health or social care or treatment or the management of health or social care systems and services pursuant to contract with a health professional". In order to protect the vital interests of a Student/ Resident.

• Address • Telephone numbers • Next of kin data • Career history • Bank details • Education history • Occupational health details • DBS data including prove of address, passport, driving licence • Birth certificate • CCTV footage	Employees	Recording information of all company employees, paying employees, processing payments, storing bank and financial information.	Keeping accurate records of company employees, paying employee, reporting to HMRC and performance of contract with employees	Employees & contractors who are not employees, for example pension providers, health care agencies, life assurance companies, HMRC and banks.	8 years after leaving employment CCTV footage is systematically deleted every five weeks, unless a request to view images (by, for example, the police) is received before the 5 week period has expired.	Performance of the employee's contract of employment. Legal basis: for tax, accounting, retirement scheme purposes. In order to protect the vital interests of a Student/ Resident.

• Address • Telephone numbers • Next of kin data • Career history • Bank details • Education history • Occupational health details • DBS data including prove of address, passport, driving licence • Birth certificate	Prospective Employees	Recording and reviewing information relating to prospective employees.	Assessing the suitability of a prospective employee for an available role within the company.	Employees	6 months after the interview.	Legitimate Interest: recruiting employees and selecting the most suitable candidates for roles within the company

• Name • Job Title • Address • DBS details • References • Data subject's Bank details • CCTV footage	Contractors such as therapists and consultants	Recording and reviewing information in relation to the purchase of specialist services	Assessing the suitability of a prospective contractors and third parties for work within the organisation.	Employees	8 years after contract end CCTV footage is systematically deleted every five weeks, unless a request to view images (by, for example, the police) is received before the 5 week period has expired.	Legitimate Interest: selecting the most suitable contractors and third parties for roles within the company In order to protect the vital interests of a Student/ Resident.

• Name • Address • Bank details • Family details • Medical history • Date of Birth	Parents and next of kin of students and residents	Planning and reviewing care and education Updating records as details change	To ensure that students and resident are well cared for and well educated To keep people safe	Employees and Third Party Staff Support staff, education staff and management can access student / resident details within their location. Finance staff can access some of the detail from perspective of managing accounts Compliance team can access details when carrying out audits / internal inspections Local authorities and referring partners, carry out audits receive reports and exit information Ofsted and CQC review details during statutory inspections.	In relation to a child student/ resident: 75 years from the last date of entry. This is a required in order to comply with the Care Act the Mental Capacity Act and the Children's Home Regulations. For adults: 20 years from the last date of entry.	Consent from a data subject. Fulfilment of a contract with a local authority or referring partner

Document equality impact assessment – part A

Document Title	Data Protection
Name of person completing equality impact assessment:	Debra Fullerton
Date equality impact assessment completed:	25th April 2023

Characteristics	Impact		Equality Impact Assessment form completed?
	Yes	No	
Age		x	If ***No*** comment: The policy applies equally to individuals regardless of their personal characteristics
Disability		x	
Ethnicity		x	
Gender		x	
Religion or belief		x	
Sexual orientation		x	
Socio-economic		x	
Gender Reassignment		x	
Maternity/Pregnancy		x	
Marriage/Civil Partnership		x	

Equality target group	a) Positive impact		b) Negative impact		Reason/comment
	High	Low	High	Low	
None					

Document equality impact assessment – part B

What is the main purpose or aims of the policy	
To inform people how Kisimul will collect, store and protect their data and to explain to people their rights in law	
Who will be the beneficiaries of this policy?	
People that work for and with Kisimul. People that are cared for and educated by Kisimul.	
Has the policy been explained to those it might affect directly or indirectly?	
Yes	
Have you consulted on this policy?	
Yes – submitted to PESC for discussion and ratification	
What are the expected outcomes of this policy?	
That people know their rights with regard to their personal data and Kisimul has systems and processes in place to protect peoples' personal data	
Name of person completing equality impact assessment:	Debra Fullerton

Document change log

The document change log acts as a register of all authorised changes made to this document.

Changes will not be made unless authorised by the document owner.

Description of change	Change made by	Date document republished