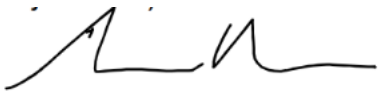
KORU CIC

DATA PROTECTION POLICY

Author Signature: 

February 2026

Approved: Andrea Micah CEO Of the KORU Project

Signed approved: 

Introduction and scope

This policy outlines The Koru Project's (also referred to as 'Koru') commitment to data protection and compliance with the UK Data Protection Act 2018. The purpose of this policy is to ensure that all personal data held by the company is processed lawfully, fairly, and transparently, and that the rights of data subjects are protected. This policy applies to all individuals working on behalf of The Koru Project, including trustees, staff, and volunteers.

Data Protection Lead

The Koru Project has a Data Protection Lead - Andrea Micah, CEO who will be responsible for overseeing data protection and leading on any incident investigation and reporting. The Data Protection Lead will also ensure that all staff and volunteers are provided with any induction, on the job or other training and made aware of their data protection responsibilities.

Data Protection

Data protection is the practice of safeguarding personal information by applying data protection principles and complying with the Data Protection Act. The Data Protection Act is a UK law that regulates the processing of personal data. The UK Information Commissioner's Office (ICO) provides guidelines on data protection that The Koru Project will follow.

UK GDPR: The UK General Data Protection Regulation, which outlines the rules for processing personal data in the UK.
Data Processor: An individual or organisation that processes personal data on behalf of a data controller.
Data Controller: An individual or organisation that determines how and why personal data is processed.
Data Subject: An individual whose personal data is being processed.
Processing: Any operation performed on personal data, including collection, storage, use, and disclosure.
Personal Data: Any information that can identify a living individual, such as name, address, or email address.
Sensitive Personal Data: Personal data that requires extra protection, such as health information or ethnic origin.
Direct Marketing: Any communication aimed at promoting a product or service directly to an individual.
PECR: The Privacy and Electronic Communications Regulations, which govern electronic direct marketing.
Valid Consent: Consent given freely, specifically, and informed, and can be withdrawn at any time.
Legitimate Business Purpose: A lawful reason for processing personal data that is necessary for the legitimate interests of the data controller or a third party.

Data Protection Principles

Data is: Processed lawfully, fairly and in a transparent manner.

There are several grounds on which data may be collected, including consent.

We are clear that our collection of data is legitimate, and we have obtained consent to hold an individual's data, where appropriate.

We are open and honest about how and why we collect data and individuals have a right to access their data.

We only collect data for specified, explicit and legitimate purposes and will not use for any other purpose.

When data is collected for a specific purpose, it may not be used for any other purpose, without the consent of the person whose data it is.

We collect all the data we need to get the job done and none that we don't need.

We ensure that what we collect is accurate and have processes and/or checks to ensure that data which needs to be kept up-to-date is, such as beneficiary, staff or volunteer records.

We correct any mistakes promptly.

We only hold data only for as long as we need to - including both hard copy and electronic data. Some data must be kept for specific periods of time (e.g. accounting records, Health and Safety records).

We have a process that ensures data no longer needed is destroyed through annual policy reviews and regular administrative checks.

We follow the ICO guidance on data storage, sharing and security.
Data is held securely, so that it can only be accessed by those who need to do so. For example, paper documents are locked away, access to online folders in shared drives is restricted to those who need it, IT systems are password protected, and/or sensitive documents that may be shared (e.g. payroll) are password protected.

Data is kept safe. Our IT systems have adequate anti-virus and firewall protection that's up-to-date. Staff understand what they must and must not do to safeguard against

cyber-attack, all staff undertake cyber security training and understand the importance of keeping data safely and securely.

Data is recoverable. We have adequate data back-up and disaster recovery processes.

Individual Rights

We recognise that individuals' rights include the right to be informed, of access, to rectification, erasure, restrict processing, data portability and to object.

Use of imagery/video

All imagery is protected by copyright and cannot be used without the consent of the owner, usually the person who took the image. The Koru Project seek consent from all individuals in images. Particular care is taken when using images of children or other vulnerable people where an image consent form would be used.

The Koru Project adhere to the following principles for use of imagery:

- If an image is taken for one purpose, such as personal use, it cannot be used for another without the consent of the individuals concerned.
- If the image is sensitive personal data, we ensure we have the individual's consent.
- For small groups and individuals, an image consent form is used.
- When using images of children, or people who may not be competent, we either have valid consent or do not take an image of that person in the first place.
- When using images of children or other vulnerable people, we do not use the image where it could place an individual at risk. Particularly, if it is to be used publicly, such as in the Media or on the web.

- When photographing large groups, individuals are given a chance to opt out of the photograph, and we do not include any individuals where there may be any risk to them.

- We only use the image according to how the person/people were told it would be used. If there is a question over this, the image would be discounted for use.

Data breach

A breach is more than only losing personal data. It is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

We will investigate the circumstances of any loss or breach, to identify if any action needs to be taken. Action might include changes in procedures, where there will help to prevent a re-occurrence or disciplinary or other action, in the event of negligence.

We will notify the ICO within 72 hours of a breach if it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals.

For example:

- Result in discrimination.
- Damage to reputation.
- Financial loss.
- Loss of confidentiality or any other significant economic or social disadvantage.

Data Protection complaints

In line with the ICO's guidance and the Data (Use and Access) Act 2025, we have a dedicated process for handling complaints relating to personal data. Anyone who believes we have not handled their personal information appropriately may raise a data protection complaint with us.

We will:

- Provide a clear and accessible way for individuals to submit data protection complaints.
- Acknowledge receipt of such complaints within 30 calendar days.
- Take appropriate steps to investigate the complaint without undue delay, including making necessary enquiries and keeping the complainant informed throughout.
- Communicate the outcome of the complaint promptly and clearly, explaining any actions taken or decisions made.

All complaints will be handled fairly, transparently, and in accordance with our obligations under the Data Protection Act. If the complainant remains dissatisfied, they may escalate the matter to the Information Commissioner's Office (ICO).

Other Policies

The Koru Project also reference Data Protection within our Safeguarding policy and Privacy policy. Separate Data Protection and GDPR information is given to all clients receiving therapy so they can understand the way their data is handled and give informed consent for The Koru Project to obtain, process and store their data accordingly. This policy should be read in conjunction with our Privacy policy.

Children

People under 13 years of age are not legally able to give consent. We ensure that privacy notices, or other information given to them, are written and presented in a way that is understandable and fair. A responsible adult is always given a copy of this policy alongside information given to children.

People who are not competent

Some people may be unable to give consent, and this must be obtained from the person who is able to make decisions on their behalf, such as a Lasting Power of Attorney. Any decisions that we may make on their behalf are always taken to be in their best interests.

Vulnerable groups

When we work with people who may be particularly at risk, we include additional provisions to protect them. Examples include adults and children who are refugees, asylum seekers or those in the criminal justice system. In these instances, we only store any personal information where there are clear grounds for doing so in order that work can be safely carried out. We work closely with trusted partners including local authorities and registered charities who act as the data controllers for vulnerable groups.

Special Category Data

Special category (sensitive) data is more sensitive and so needs more protection. For example, information about an individual's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life or sexual orientation.

Subject Access Request

Koru understands that by law, people can ask for a copy of any information that's to do with them and this constitutes a Subject Access Request (SAR). If a SAR is made by phone, in person, or in writing, Koru has guidelines to ensure the SAR is handled within 28 days and by a staff member who is trained to understand how to deal with this data appropriately.

International Data Transfers

We comply with the ICO guidance when transferring data to another country.

Privacy and Electronic Communications

Known as PECR, there are special regulations covering electronic marketing messages (by phone, fax, email or text), cookies and electronic communication services to the public. We carry out an annual review to ensure our PECR are relevant and compliant with the Data Protection Act.

Fundraising

We will ensure that our fundraising complies with the Data Protection Act and ICO guidelines and also the Fundraising Regulator guidelines including, if applicable, direct marketing and PECR. We will respect the privacy and contact preferences of our donors. We will respond promptly to requests to cease contacts or complaints and act to address their causes.

Artificial Intelligence

We have adopted and comply with the Organisation AI Ethics & Governance Framework and ICO AI guidance. If AI has access to data sets containing personal information, such as staff or beneficiary records, we have carried out an AI Risk Analysis and a data protection impact assessment (DPIA) and updated our data protection policy and procedures to reflect this.

Data Retention

Our data will only be kept for as long as there is an administrative need to do so in order to enable our organisation to carry out its business or support functions, or for as long as it is required to demonstrate compliance for audit purposes or to meet legislative requirements.
In general, records are kept for 6 years after the end of the accounting year to which they relate but we do not keep personal records any longer than necessary and certain records may be required to be retained for longer. Factors affecting retention periods include legal requirements, storage costs, historical value, industry standards, and archival needs.

Policy approval and review

Version No	Approved By	Approval Date	Main Changes	Review Period
1.0	Board	Feb 2026		Annually