



KORI DATA PROTECTION POLICY

This policy sets out the obligations of KORI regarding data protection and the rights of customers, contacts, freelancers, employees, trustees, volunteers, participants, supporters, donors, and any other data subjects engaged with the Charity in respect of their personal data, under Data Protection Legislation such as the Data Protection Act (DPA) 2018.

It also sets our obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be always followed by KORI, its freelancers, employees, trustees, volunteers, agents, contractors, or any other parties working on behalf of KORI.

KORI is registered with the Information Commissioner's Office registration reference **CSN5300185**. As a Controller of personal data, KORI recognises its duty to ensure that all such data is always handled properly and confidentially, irrespective of whether it is held on paper or by electronic means and covers its whole lifecycle. The CEO has delegated authority supported by the Trustees for the implementation of this policy.

Data Owner – is the person or entity which can authorise or deny access to certain data and is responsible for its accuracy and integrity.

Data Subject – the individual who is the subject of personal and sensitive information. NB: the data protection act does not count as a data subject a deceased individual or an individual who cannot be distinguished from others.

Personal Data - any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Data Controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor – a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Personal Information - information that identifies someone as an individual, such as:

- personal details / family details / lifestyle and social circumstances / financial details / education and employment / visual images

Sensitive Personal Information - information about:

- physical or mental health details / racial or ethnic origin / religious or other beliefs of a similar nature / offences and alleged offences / criminal proceedings, outcomes, and sentences

Data protection principles

The Data Protection Act (DPA) 2018 regulates the data processing relating to living and identifiable individuals. This includes the obtaining, holding, using, or disclosing of such information, and covers computerised records as well as manual filing systems.

The principles apply to “personal and sensitive personal data” from which the subjects of that data are identifiable. KORI freelancers, employees, volunteers, and trustees who process, use, or have access to any personal information in the course of their duties, will ensure that these principles are always followed.

KORI data users must comply with the data protection principles of good practice which underpin the Data Protection Act. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. KORI follows the Data Protection Principles outlined in General Data Protection Regulation, which are summarised below:

- Personal data will be processed fairly, lawfully and in a transparent manner
- Data will only be collected and used for specified, explicit and legitimate purposes.
- Data will be adequate, relevant, and not excessive.
- Data will be accurate and up to date.
- Data will not be held any longer than necessary.
- Data subject's rights will be respected.
- Data will be kept safe from unauthorised access, accidental loss, or damage.
- Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.
- Data will not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

Rights of data subjects: DPA 2018 provides the following rights for individuals:

- The Right to Be Informed: KORI's Data Protection Officer can be contacted by:
 - Email: info@kori.org.uk
or
 - Post: marked FAO Data Protection Officer, Odiri Ighamre, London, N11 2EZ
 - The Data Protection Officer is the C.E.O who is responsible for overseeing the implementation of this policy and for monitoring compliance with this policy and any other KORI linked policies & procedures.

KORI keeps secure records of all personal data collection, holding and processing, which incorporates the following information:

- The name and details of KORl, its Data Protection Officer, and any applicable third-party data processors.
- The purposes for which KORl collects, holds and processes personal data
- Details of the categories of personal data collected, held, and processed by KORl and the categories of data subject to which that personal data relates.
- Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards.
- Details of how long personal data will be retained by KORl.
- Detailed descriptions of all technical and Organisational measures taken by KORl to ensure the security of personal data.

Keeping Data Subjects Informed (Privacy Rights): KORl has an overarching and organisational Consent & Privacy document that underpins all departmental privacy notices. Privacy notices are the best way for us to tell individuals (e.g., customers, freelancers, staff, volunteers, trustees etc.) why and how we use personal and sensitive information. The notices are used to share the specific detail on personal data processes that we have in place across individual departments and teams.

KORI will:

- Where personal data is collected directly from data subjects, they will be informed of its purpose at the time of collection.
 - Inform data subjects of data purposes at the time of collection when personal data is collected dire.
- Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose normally at the time of sharing or as soon as reasonably possible after the personal data is obtained.

The following information will be provided, usually in privacy notices:

- The purpose(s) for which the personal data is being collected and will be processed and the legal basis justifying that collection and processing.
- Where applicable, the legitimate interests upon which KORl is justifying its collection and processing of the personal data.

- Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed.
- Where the personal data is to be transferred to one or more third parties, details of those parties.
- Details of data retention.
- Details of the data subject's rights under Data Protection Legislation.
- Where applicable, details of the data subject's right to withdraw their consent to KORI processing their personal data at any time.
- Details of the data subject's right to complain to the Information Commissioner's Office, the regulator.
- Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data.
- Where applicable, details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions and any consequences.

1. The Right of Access (Subject Access Requests): Data subjects may make Subject Access Requests (SAR) at any time to find out more about the personal data which KORI holds about them, what we are doing with that personal data and why. Anyone wishing to make a SAR must complete the Subject Access Request Form and send to KORI's Data Protection Officer by:

- Email: info@kori.org.uk
- or
- Post: marked FAO Data Protection Officer, London N11 2EZ.

Responses shall normally be made within 30 calendar days of receipt. If additional time is required, the data subject will be notified. All enquiries or complaints received shall be handled by the Data Protection Officer who will be supported by trustees when requested.

2. The Right to Rectification Data subjects have the right to rectify any of their personal data that is inaccurate or incomplete. We will rectify the personal data in question and inform the data subject of that rectification, as quickly as possible, but within one month of the data subject informing KORI of the issue.

If any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data

record and will be asked to confirm the changes have been appropriately amended.

3. The Right to Erasure ('the right to be forgotten') Data subjects have the right to request that KORI erases the personal data we hold about them in the following circumstances:

- It is no longer necessary for us to hold that personal data with respect to the purpose(s) for which it was originally collected or processed.
- The data subject wishes to withdraw their consent to KORI holding and processing their personal data.
- The data subject objects to KORI holding and processing their personal data (and there is no overriding legitimate interest to allow KORI to continue doing so)
- The personal data has been processed unlawfully.
- The personal data needs to be erased for KORI to comply with a particular legal obligation.
- The personal data is being held and processed for the purpose of providing information services to a child.

4. Unless KORI has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with and the data subject informed of the erasure, within 30 calendar days of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed. If any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the need for erasure (unless it is impossible or would require disproportionate effort to do so).

5. The Right to Restrict Processing Data subjects may request that we cease processing the personal data we hold about them. If a data subject makes such a request, KORI will retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further. If any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

6. The Right to Data Portability Business processes should allow individuals to move, copy or transfer their personal data from one environment to another in a safe and secure way, without any hindrance to the usability of the data.

The right to data portability only applies when each of the following are met:

- The personal data an individual has provided to a controller.
- Where the processing is based on the individual's consent or the performance of a contract.
- When processing is carried out by automated means. ('Processing by automated means' is defined as personal data processed electronically, for example on a computer, smart phone, or call recording software).

7. The Right to Object Data subjects have the right to object to KORI processing their personal data based on legitimate interests, direct marketing (including profiling) and processing for scientific and/or historical research and statistics purposes. Where a data subject objects to KORI processing their personal data based on our legitimate interests, we will cease such processing immediately, unless it can be demonstrated that KORI has legitimate grounds for such processing override the data subject's interests, rights, and freedoms or that the processing is necessary for the conduct of legal claims. Where a data subject objects to KORI processing their personal data for direct marketing purposes, KORI shall cease such processing immediately.

8. Rights with Respect to Automated Decision Making and Profiling: KORI does not usually use personal data in any automated decision-making processes. Where such decisions have a legal (or similarly significant effect) on data subjects, those data subjects have the right to challenge such decisions, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from KORI. The right described above does not apply in the following circumstances:

- The decision is necessary for entry into, or the performance of, a contract between KORI and the data subject.
- The decision is authorised by law; or the data subject has given their explicit consent.
- KORI may use personal data for profiling purposes. When personal data is used for profiling purposes, the following shall apply:

- Clear information explaining the profiling shall be provided to data subjects, including the significance and likely consequences of the profiling.
- Appropriate mathematical or statistical procedures shall be used.
- Technical and organisational measures shall be implemented to minimise the risk of errors. If errors occur, such measures must enable them to be easily corrected; and All personal data processed for profiling purposes shall be secured to prevent discriminatory effects arising from profiling.

9. DATA SECURITY: KORI will ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

- Personal data must never be included within the subject line or message body of an email.
- All personal data documents legitimately transmitted via IT systems (e.g., email) will be protected using a strong password and marked “confidential”.
- Personal data may be transmitted over secure networks only. Transmission over unsecured networks is not permitted in any circumstances.
- Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email, and stored securely. The email itself should be deleted. All temporary files associated must also be deleted.
- Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using Special Delivery post and all personal data to be transferred physically, whether in hardcopy form or on removable electronic encrypted media shall be transferred in a suitable container marked “confidential”.

KORI will ensure that the following measures are taken with respect to the storage of personal data:

- All electronic copies of personal data should be stored securely either by using passwords or restricted permissions on folders.
- All hard copies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar.

- All personal data stored electronically should be backed up daily with backups encrypted and stored offsite.
- No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to KORI or otherwise without approval of the appropriate member and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is necessary.
- No personal data should be transferred to any personal device belonging to an employee, and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of KORI where the party in question has agreed to comply fully with this policy and all Data Protection Legislation (which may include demonstrating to KORI that all suitable technical and organisational measures have been taken).
- When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. (If unsure individuals are required to discuss this with the KORI Team)

KORI shall ensure that the following measures are taken with respect to the use of personal data:

- Personal data processed by KORI must only be used for the purpose it was collected for.
- No personal data may be shared informally and/or transferred to an employee, trustees, freelancers, volunteers, agent, sub-contractor, or other party working on behalf of KORI. If they require access to any personal data that they do not already have access to, such access should be formally requested from the relevant member of the team.
- Personal data must be always handled with care and should not be left unattended or on view to unauthorised employees, trustees, volunteers, agents, sub-contractors, or other parties at any time.
- Where personal data held by KORI is used for marketing purposes, it shall be the responsibility of the nominated person to ensure that the appropriate consent is obtained, documented for as long as deemed necessary and that no data subjects have opted out.
- KORI shall ensure that the following measures are taken with respect to IT and information security:

- All passwords used to protect personal data do not use words or phrases that can be easily guessed or otherwise compromised.
- All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols.
- Under no circumstances should any passwords be written down or shared between any employees, trustees, freelancers, volunteers, agents, contractors, or other parties working on behalf of KORI.
- If a password is forgotten, it must be reset using the applicable method.
- All software (including, but not limited to, applications and operating systems) will be kept up to date.
- Operations staff shall be responsible for installing all security-related updates as soon as reasonably and practically possible.

KORI shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

- All employees, trustees, freelancers, volunteers, agents, contractors, or other parties working on behalf of KORI shall be made fully aware of both their individual responsibilities and KORI's responsibilities under Data Protection Legislation and under this Policy and shall be provided with a copy of this Policy
- Those who only need access to, and use of, personal data to carry out their assigned duties correctly shall have access to personal data held by KORI and will be:
 1. appropriately trained to do so.
 2. handling personal data will be appropriately supervised.
 3. required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise.
- Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed. All personal data held by KORI shall be reviewed regularly.
- Where other parties working on behalf of KORI handling personal data fail in their obligations under this Policy that party shall indemnify and hold KORI harmless against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

Data should be protected at all times; this includes practical approaches such as locking away laptops when not in use and being careful who has access to where data is stored. Any loss of personal data is a security breach and all breaches, near-misses and incidents must be reported immediately to KORI's Data Protection Officer by email to info@kori.org.uk If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after being made aware of it. If a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Data Protection Officer will ensure that all affected data subjects are informed of the breach directly and without undue delay.

Data breach notifications will include the following information:

- The categories and approximate number of data subjects concerned.
- The categories and approximate number of personal data records concerned.
- The name and contact details of KORI's Data Protection Officer.
- The likely consequences of the breach.
- Details of the measures taken, or proposed to be taken, by KORI to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

Training: It is the aim of KORI that all staff will be fully informed of their Data Protection obligations and as a minimum we will provide annual training. An online tutorial is included in new starter inductions. Periodic refresher sessions are also undertaken from time to time and additional training can be.

Responsibilities Trustees:

Overall responsibility for a policy which ensures compliance with the relevant statutes Chief Executive:

- Development and maintenance of such procedures as are necessary to ensure implementation of the policy.
- Maintenance of the policy.

- Design of procedures.
- Implementation of procedures.
- Dissemination throughout their team.
- Ensuring day-to-day operational compliance.
- Reporting to the Executive Team.
- Reporting data incidents and near misses to the Data Protection Officer Individual

This Policy will have a formal review annually, if any aspect is found to be inadequate, the Policy will be reviewed earlier.

Document Name: KORI Data Protection Policy

March 2024 By: *Odiri Ighamre*