Data Protection Policy

This policy applies to all trustees, employees, and volunteers.

Statement of Intent

KidsBank is committed to a policy of protecting the rights and privacy of individuals. KidsBank needs to collect and use certain types of data to carry out our work. We recognise the importance of the correct and lawful treatment of personal data.

All personal data, whether it is held on paper, on computer or other media, will be subject to the appropriate legal safeguards and good practice as specified in the General Data Protection Regulation 2018. KidsBank will remain the Data Controller for the information held. KidsBank and volunteers will be personally responsible for processing and using personal information in accordance with the GDPR.

We fully endorse and adhere to the eight principles of the GDPR. These principles specify the legal conditions that must be satisfied in relation to obtaining, handling, processing, transportation, and storage of personal data. Trustees, staff, and volunteers running KidsBank who have access to personal information, will be expected to read and comply with this policy.

The Policy

What information is being collected?
We collect information such as your name, contact details and that required to fulfil a referral.

Who is collecting it?
KidsBank

How is it collected?
The information is collected by the completion of forms, either manually or electronically, by (or on behalf of by a qualified professional) the person the data relates to.

Why is it being collected and how will it be used?
For the administration of the charity, for communication with you and for statistical analysis.

Who will it be shared with?
KidsBank trustees, staff, and volunteers only.

Purpose

The purpose of this policy is to set out KidsBank's commitment and procedures for protecting personal data. KidsBank regards the lawful and correct treatment of

personal information as very important to successful working, and to maintaining the confidence of those whom we deal with.

- We want to collect limited personal information of clients to fulfil a referral request.
- We want to collect personal information from our referral partners and volunteers so that our service ensures good communication.
- We want to claim gift aid on a person's donations.
- We want to maintain accurate records of clients in order to anonymise data to use in funding applications and publicity.
- We want to use the limited personal data we collect and store for 5 years before anonymising for long term use in order to assess the impact of our services.
- We want to maintain contact information for anyone who has volunteered for KidsBank so we can contact them about future volunteering opportunities.

GDPR

In line with the GDPR principles, KidsBank will ensure that personal data will:

- Be obtained fairly and lawfully and shall not be processed unless certain conditions are met
- Be obtained for a specific and lawful purpose
- Be adequate, relevant but not excessive
- Be accurate and kept up to date
- Be held longer than necessary
- Be processed in accordance with the rights of data subjects
- Be subject to appropriate security measures

Where 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, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

The definition of 'processing' is obtaining, using, holding, amending, disclosing, destroying, and deleting personal data. This includes paper based personal data as well as that kept on computer.

The Personal Data Guardianship Code suggests five key principles of good data governance on which best practice is based. The organisation will seek to abide by this code in relation to all the personal data it processes, i.e.

- Accountability: those handling personal data follow publicised data principles to help gain public trust and safeguard personal data.
- Visibility: Data subjects should have access to the information about themselves that an organisation holds. This includes the right to have incorrect personal data corrected and to know who has had access to this data.
- Consent: The collection and use of personal data must be fair and lawful. Personal data should only be used for the purposes agreed by the data

subject. If personal data is to be shared with a third party or used for another purpose, the data subject's consent should be explicitly obtained.
- Access: Everyone should have the right to know the roles and groups of people within an organisation who have access to their personal data and who has used this data.
- Stewardship: Those collecting personal data have a duty of care to protect this data throughout the data life span.

Type of Information Processed

Some examples of Personal Data:
- Name
- Address
- Telephone number
- E-mail Address
- Family Relationship

Some examples of Sensitive Personal data:
- Gender
- Ethnic Origin
- Disability
- Marital Status

KidsBank processes the following personal information (information that allows a person to be identified):
- Volunteer and donor name, address, email and contact number
- Referrer name, email address and contact number
- Client name, email address, contact number, postcode, address (if given specifically for delivery purposes), gender and age of children, ethnicity.
- Information required by HMRC in relation to financial donations subject to Gift Aid.

Personal information may be in the form of paper copies of referral forms, or digital referral forms saved on a computer. Paper copies are held on file with a list of items provided. The file is kept in a locked box. Digital files are saved on a password protected user account.

Groups of people within the organisation who will process personal information are:
- Trustees, staff, treasurers, and volunteers.

Applying the GDPR within KidsBank

Whilst access to personal information is limited to the aforementioned staff and volunteers at KidsBank, volunteers at KidsBank may undertake additional tasks which involve the collection of personal details from members of the public.
In such circumstances we will let people know why we are collecting their data and it is our responsibility to ensure the data is only used for this purpose.

Correcting data

Individuals have a right to have data corrected if it is wrong, to prevent use which is causing them damage or distress or to stop marketing information being sent to them.

Responsibilities

KidsBank is the Data Controller under the GDPR, and is legally responsible for complying with the GDPR, which means that it determines what purposes personal information held will be used for.

The Board of Trustees will take into account legal requirements and ensure that it is properly implemented, and will through appropriate management, strict application of criteria and controls:

- Observe fully conditions regarding the fair collection and use of information,
- Meet its legal obligations to specify the purposes for which information is used,
- Collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements,
- Ensure the quality of information used,
- Ensure that the rights of people about whom information is held, can be fully exercised under the GDPR. These include:
    - The right to be informed that processing is being undertaken
    - The right of access to one's personal information
    - The right to prevent processing in certain circumstances and
    - The right to correct, rectify, block or erase information which is regarded as wrong information
- Take appropriate technical and organisational security measures to safeguard personal information,
- Ensure that personal information is not transferred abroad without suitable safeguards,
- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information,
- Set out clear procedures for responding to requests for information

The Data Protection Officer reporting to the Board of Trustees is the CEO.

The Data Protection Officer will be responsible for ensuring that the policy is implemented and will have overall responsibility for:

- Ensuring that everyone processing personal information understands that they are contractually responsible for following good data protection practice
- Ensuring that everyone processing personal information is appropriately trained to do so
- Ensuring that everyone processing personal information is appropriately supervised
- Ensuring that anybody wanting to make enquiries about handling personal information knows what to do
- Dealing promptly and courteously with any enquiries about handling personal information

- Describing clearly how KidsBank handles personal information
- Regularly reviewing and auditing the ways KidsBank holds, manages and uses personal information
- Regularly assessing and evaluating KidsBank's methods and performance in relation to handling personal information
- Ensuring that all staff and volunteers are aware that a breach of the rules and procedures identified in this policy may lead to action being taken against them

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the GDPR.
In case of any queries or questions in relation to this policy please contact the Data Protection Officer.

Training

Training and awareness raising about the GDPR and how it is followed in this organisation will take the following forms:
On induction: all volunteers are given a copy of our data protection policy and asked to sign the Volunteers' Agreement to show they have read and understood it. Only the Data Protection Officer has access to passwords and locked files.

Data collection

Before personal information is collected, we will consider:

- What information we need in order to deliver our service efficiently
- What information we need in order to show the impact of our service
- How long we will keep the information on record:
    - We will keep data on clients for a maximum of 5 years from the client's last use of our service.
    - We will keep volunteer data for 1 year after their last contact with us, then it will be deleted.
    - We will keep data on Gift Aid declarations for 6 years, in accordance with HMRC regulations.
    - Anonymised data and aggregate totals will be maintained beyond the destruction of individual records so we can assess the impact of our services.

We will inform people whose information is gathered about the following:

- That we need key information in order to deliver our service
- That the information provided will be held securely
- That by completing the referral form, they consent to KidsBank using the anonymised data.
- That by completing the referral form, they consent to being contacted in order for us to carry out our service such as making an appointment, delivery, product recall, out of stock items.
- That staff will have relevant financial and personal information held in order to enable KidsBank to meet legal and contractual obligations.

Data Security

Once received, all correspondence containing 'personal' or 'sensitive personal' data must immediately be either securely processed, stored, or destroyed; or immediately passed on to another member of staff or a volunteer for secure processing, storing or destruction.

- No visible, unattended data

All versions of any 'personal' or 'sensitive personal' data must be handled in a timely and secure fashion and at no time left unattended.

- Electronic Copies

Electronic copies should at no time left open and unattended on a computer monitor, and never should be unnecessarily distributed.

Computer screens should be locked if they are left unattended for any time.
All electronic correspondence containing 'personal' or 'sensitive personal' data should be deleted, and then deleted from any electronic 'trash' bin once it has been processed.

- Paper Copies

Paper copies should exist in only one of three states; being securely processed, being securely stored, or being securely destroyed.
The organisation will take steps to ensure that personal data is kept secure, at all times, against unauthorised or unlawful loss or disclosure. The following measures will be taken:

- All referrals are emailed to a secure email address which only team members have access to or supplied direct to team members as paper copies and then stored in a locked file.
- Any paper copies of volunteer agreements are kept in a locked file.
- A record of the DBS numbers registered.

Data Breach
Any unauthorised disclosure of personal data to a third party may result in disciplinary action being taken.
The trustees are accountable for compliance of this policy. A trustee could be personally liable for any penalty arising from a breach that they have made.
Any unauthorised disclosure made by a volunteer may result in the termination of the volunteering agreement.
If a volunteer or member of staff is made aware of a data breach they should notify the Data Protection Officer.
Any serious data breaches or data loss will be reported to the Information Commissioners Office and the Charity Commission. This includes:

- Charity data that has been accessed by an unknown person and/or deleted.
- A charity device, containing personal details of beneficiaries or staff, has been stolen or gone missing and it's been reported to the police;
- Charity funds lost due to an online or telephone 'phishing scam', where trustees were conned into giving out bank account details;
- A Data Protection Act breach has occurred and been reported to the ICO.

Data Subject Access Requests

Anyone whose personal information we process has the right to know:

- What information we hold and process on them
- How to gain access to this information
- How to keep it up to date
- What we are doing to comply with the Act.

They also have the right to prevent processing of their personal data in some circumstances and the right to correct, rectify, block or erase information regarded as wrong.

Individuals have a right under the Act to access certain personal data being kept about them on computer and certain files. Any person wishing to exercise this right should apply in writing address FAO the CEO to info@kidsbankchester.com.

The following information will be required before access is granted:

- Full name and contact details of the person making the request
- Relationship with the organisation and applicable timescales

We may also require proof of identity before access is granted. The following forms of ID may be required: passport, birth certificate.

Queries about handling personal information will be dealt with swiftly and politely. We will aim to comply with requests for access to personal information as soon as possible but will ensure it is provided within the 28 days required by the GDPR from receiving the written request.

Disclosure

KidsBank may need to share data with other agencies such as the local authority, funding bodies and other voluntary agencies.
The data subject will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows KidsBank to disclose data (including sensitive data) without the data subject's consent.
These are:

- Carrying out a legal duty or as authorised by the Secretary of State
- Protecting vital interests of a data subject or other person
- The data subject has already made the information public
- Conducting any legal proceedings, obtaining legal advice or defending any legal rights
- Monitoring for equal opportunities purposes – i.e. race, disability or religion
- Providing a confidential service where the data subject's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. a safeguarding concern for the welfare of a child or adult

KidsBank regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.

Risk Management

The consequences of breaching Data Protection can cause harm or distress to service users if their information is released to inappropriate people, or they could be denied a service to which they are entitled. Volunteers should be aware that they can be personally liable if they use clients' personal data inappropriately. This policy is designed to minimise the risks and to ensure that the reputation of KidsBank is not damaged through inappropriate or unauthorised access and sharing.

Further information

If members of the public/or stakeholders have specific questions about information security and data protection in relation to KidsBank please contact the Data Protection Officer.

The Information Commissioner's website (www.ico.gov.uk) is another source of useful information.