



THE GENERAL DATA PROTECTION REGULATION (GDPR) POLICY

Introduction

The purpose of this policy document is to establish a clear and agreed understanding of what GDPR means within KidsAid to encourage uniformity in practice and ensure that service users know what they can expect from this organisation.

KidsAid will ensure that all personal data held will be:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant, and limited to what is necessary.
- Accurate and kept up to date.
- Kept in a form which permits identification of data subjects for no longer than is necessary.
- 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.

Data Protection Policy

Under the EU General Data Protection Regulations (GDPR) KidsAid is required to comply with the GDPR and undertakes to do so.

Throughout this policy document, numbers prefixed by 'Article' in brackets (*e.g.*: (Article:5)) refer to the relevant Article(s) in the GDPR framework and for ease of access, extracts of relevant GDPR Articles are contained in the Appendix to this Policy.

Definitions

Data Subject

A data subject is an identifiable individual person about whom KidsAid holds personal data.

Contact Information

For the purposes of this Policy, “contact information” means any or all the person’s full name, full postal address, telephone and/or mobile number and social media IDs/usernames (e.g., Facebook, WhatsApp etc.)

Principles of the GDPR

- KidsAid will ensure that all personal data that it holds will be:
- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Further processing for archiving or statistical purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be incompatible with the initial purposes.
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; 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 subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- 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.

Lawful Processing

KidsAid will obtain, hold, and process all personal data in accordance with the GDPR for the following lawful purposes. In all cases the information collected, held, and processed will include contact information (as defined above).

By Consent

- People who are interested in, and wish to be kept informed of, the activities of KidsAid.
- Subject to the person’s consent, this may include information selected and forwarded by KidsAid on activities relevant to those of the charity by other organisations. Note: This will not involve providing the person’s personal data to another organisation.

The information collected may additionally contain details of any particular areas of interest about which the person wishes to be kept informed.

The information provided will be held and processed solely for the purpose of providing the information requested by the person.

By Contract

People who sell goods and/or services to, and/or purchase goods and/or services from KidsAid.

The information collected will additionally contain details of:

- The goods/services being sold to or purchased from KidsAid.
- Bank and other details necessary and relevant to the making or receiving of payments for the goods/services being sold to or purchased from KidsAid.

The information provided will be held and processed solely for the purpose of managing the contract between KidsAid and the person for the supply or purchase of goods/services.

By Legal Obligation

People where there is a legal obligation on KidsAid to collect, process and share information with a third party e.g., the legal obligations to collect, process and share with HM Revenue & Customs payroll information on employees of KidsAid.

The information provided will be held, processed, and shared with others solely for the purpose meeting KidsAid's legal obligations.

- Taxation (HM Revenue & Customs): to manage an employee's PAYE and other taxation affairs the information collected will additionally contain details, as required by HM Revenue & Customs, of:
 - The person's National Insurance Number.
 - The person's taxation codes.
 - The person's salary/wages, benefits, taxation deductions & payments.
 - Such other information as may be required by HM Revenue & Customs.
- Pensions: to manage an employee's statutory pension rights the information collected will additionally contain details, as required by KidsAid's pension scheme (National Employees Savings Trust, NEST), of:
 - The person's National Insurance Number.
 - The person's salary/wages, benefits, taxation & payments.
 - Such other information as may be required by the NEST scheme.

By Vital Interest

KidsAid undertakes no activities which require the collection, holding and/or processing of personal information for reasons of vital interest.

By Public Task

KidsAid undertakes no public tasks which require the collection, holding and/or processing of personal information.

Legitimate Interest

- Volunteers, Including Trustees: to be able to operate efficiently, effectively, and economically, it is in the legitimate interests of KidsAid to hold such personal information on its volunteers and trustees as will enable KidsAid to communicate with its volunteers on matters relating to the operation of the charity, e.g.:
 - The holding of meetings.
 - Providing information about the KidsAid's activities – particularly those activities which, by their nature, are likely to be of particular interest to individual volunteers/trustees.
 - Seeking help, support, and advice from volunteers/trustees, particularly where they have specific knowledge and experience.
- Ensuring that any needs of the volunteer/trustee are appropriately and sensitively accommodated when organising meetings and other activities of KidsAid.

Individual Rights

The following clauses are taken primarily from the guidance provided by the Office of the Information Commissioner:

<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/>

The Right to be Informed (Articles 12-14)

When collecting personal information, KidsAid will provide to the data subject advice written in clear and plain language which is concise, transparent, intelligible, and easily accessible containing the following information:

- The identity and contact details of the CEO.
- Purpose of the processing and the lawful basis for the processing.
- The legitimate interests of the CEO or third party, where applicable.
- Categories of personal data.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to third country and safeguards.
- Retention period or criteria used to determine the retention period.
- The existence of each of data subject's rights.
- The right to withdraw consent at any time, where relevant.
- The right to lodge a complaint with a supervisory authority.
- The source the personal data originates from and whether it came from publicly accessible sources.

- Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data.
- The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences.

In the case of data obtained directly from the data subject, the information will be provided at the time the data are obtained.

In the case that the data are not obtained directly from the data subject, the information will be provided within a reasonable period of KidsAid having obtained the data (within one month), *or*, if the data are used to communicate with the data subject, at the latest, when the first communication takes place; *or* if disclosure to another recipient is envisaged, at the latest, before the data are disclosed.

The Right of Access (Article: 15)

The data subject shall have the right to obtain from KidsAid confirmation as to whether or not personal data concerning him/her are being processed, and, where that is the case, access to his/her personal data and the information detailed in the KidsAid's relevant Privacy Policy.

The Right to Rectification (Article: 16)

The data subject shall have the right to require the CEO without undue delay to rectify any inaccurate or incomplete personal data concerning him/her.

The Right to Erase (the right to be forgotten) (Article: 17)

Except where the data are held for purposes of legal obligation or public task (0 or 0) the data subject shall have the right to require KidsAid without undue delay to erase any personal data concerning him/her. Note: This provision is also known as "The right to be forgotten".

The Right to Restrict Processing (Article: 18)

Where there is a dispute between the data subject and KidsAid about the accuracy, validity or legality of data held, the data subject shall have the right to require a cease of data processing for a reasonable period of time to allow the dispute to be resolved.

The Right to Data Portability (Article: 20)

Where data is held for purposes of consent or contract, the data subject shall have the right to require KidsAid to provide him/her with a copy in a structured, commonly used and machine-readable format of the data which he/she has provided to KidsAid and have the right to transmit those data without hindrance.

The Right to Object (Article: 21)

The data subject shall have the right to object, on grounds relating to his or her situation, at any time to processing of personal data concerning him/her, which is based Public Task or Legitimate Interest, including profiling based on those provisions.

KidsAid shall no longer process the personal data unless they demonstrate compelling legitimate grounds for the processing which override the interests, rights, and freedoms of the data subject or for the establishment, exercise, or defence of legal claims.

Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him/her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

Operational Policies and Procedures

Context

The Trustees of KidsAid understand and accept their responsibility under the EU General Data Protection Regulation (GDPR) to hold all personal data securely and use it only for legitimate purposes with the knowledge and approval of the data subjects.

By the following operational policies and procedures, the Trustees undertake to uphold the principles and requirements of the GDPR in a manner which is proportionate to the nature of the personal data being held by the charity. The policies are based on the Trustees' assessment, in good faith, of the potential impacts on both KidsAid and its data subjects of the personal data held by the charity being stolen, abused, corrupted, or lost.

Personnel

Data Protection Officer

In the considered opinion of the Trustees the scope and nature of the personal data held by KidsAid is not sufficient to warrant the appointment of a Data Protection Officer. Accordingly, no Data Protection Officer is appointed.

Data Controller

The Quality Lead is the Data Controller for KidsAid which is overseen by the CEO.

Data Processor

The Quality Lead is appointed the Data Processor for KidsAid.

KidsAid will not knowingly outsource its data processing to any third party (e.g., Google G-Suite, Microsoft OneDrive) except as provided for in the section "Third Party Access to Data".

Access to Data

Except where necessary to pursue the legitimate purposes of the charity, only the Quality Lead and CEO shall have access to the personal data held by the Charity.

Training

The CEO and Quality Lead will periodically undergo appropriate training commensurate with the scale and nature of the personal data that the charity holds and processes under the GDPR.

Collecting & Processing Personal Data

KidsAid collects a variety of personal data commensurate with the variety of purposes for which the data are required in the pursuit of its charitable objects.

All personal data will be collected, held, and processed in accordance with the relevant Data Privacy Policy provided to data subjects as part of the process of collecting the data.

A Data Privacy Policy is accessible on our website to all persons on whom KidsAid collects, holds, and processes data covered by the GDPR. The Data Privacy Policy provided to data subjects will detail the nature of the data being collected, the purpose(s) for which the data are being collected and the subject's rights in relation to the charity's use of the data and other relevant information in compliance with the prevailing GDPR requirements.

Information Technology

Data Protection by Design/Default

In as much as:

- None of the KidsAid Trustees are data protection professionals.
- It would be a disproportionate use of charitable funds to employ a data protection professional, given the scale and nature of the personal data held by KidsAid.
- The Trustees will seek appropriate professional advice commensurate with its data protection requirement whenever:
 - KidsAid is planning to make significant changes to the ways in which personal data is processed.
 - There is any national publicity about new risks (*e.g.*, cyber-attacks) which might adversely compromise the charity's legitimate processing of personal data covered by the GDPR.

Personal data will never be transmitted electronically (*e.g.*, by e-mail) unless securely encrypted.

Data Processing Equipment

The scale and nature of the personal data held by KidsAid is not sufficient to justify the charity purchasing dedicated computers for the processing of personal data.

Instead, KidsAid will purchase and own at least 2 and not more than 5 removable storage devices to store the personal data that it holds and processes. The removable storage devices will also act as backup devices.

Whilst the data will be processed on the computers/laptops to which the Quality Lead has access, no personal data covered by the GDPR will be stored on those computers/laptops. All interim working data transferred to such computers/laptops for processing will be deleted once processing has been completed.

When not in use the removable storage devices will be kept in a secure location and reasonably protected against accidental damage, loss, avoidable theft, or other misuse by persons other than the Quality Lead and CEO.

The Quality Lead will keep a register of:

- The location of all removable devices used for the storage and processing of personal data.
- Each occasion when the data on each device were accessed or modified and by whom.

The KidsAid's removable storage devices shall not be used for the storage of any data which are unrelated to the charity's processing of personal data.

Data Processing Location

The CEO shall only process the charity's personal data in a secure location, and not in any public place, *e.g.*, locations where the data could be overlooked by others, or the removable data storage devices would be susceptible to loss or theft.

Computers/laptops in use for data processing will not be left unattended at any time.

Data Backups

To protect against loss of data by accidental corruption of the data or malfunction of a removable data storage device (including by physical damage), all KidsAid's personal data shall be backed up periodically and whenever any significant changes (additions, amendments, deletions) are made to the data.

Backup copies of the data shall be held in separate secure locations which are not susceptible to common risks (*e.g.*, fire, flood, theft).

As far as is reasonably practical, all files containing personal data covered by the GDPR will be encrypted.

Disposal of Removable Storage Media

Equipment used to hold personal data, whether permanently or as interim working copies, which come to the end of their useful working life, or become dysfunctional, shall be disposed of in a manner which ensures that any residual personal data held on the equipment cannot be recovered by unauthorised persons.

In as much as:

- This will be a relatively infrequent occurrence.
- Techniques for data recovery and destruction are constantly evolving.
- None of the Trustees have relevant up-to-date expert knowledge of data cleansing.
- Equipment which becomes obsolete or dysfunctional shall not be disposed immediately. Instead, it will be stored securely while up-to-date expert advice on the most appropriate methods for its data cleansing and disposal can be sought and implemented.

Data Subjects

The Rights of Data Subjects

In compliance with the GDPR KidsAid will give data subjects the following rights.

These rights will be made clear in the relevant Data Privacy Policy provided to data subjects:

- The right to be informed.
- The right of access.
- The right to rectification.
- The right of erasure.
- The right to restrict processing.
- The right to data portability.
- The right to object.
- The right not to be subjected to automated decision making, including profiling.

The above rights are not available to data subjects when the legal basis on which KidsAid is holding & processing their data are:

- {SC} Subject Consent.
- {CO} Contractual Obligation.
- {LO} Legal Obligation.
- {LI} Legitimate Interest.

Rights of Access, Rectification and Erasure

Data subjects will be clearly informed of their right to access their personal data and to request that any errors or omissions be corrected.

Such access shall be given, and the correction of errors or omissions shall be made free of charge provided that such requests are reasonable and not trivial or vexatious.

There is no prescribed format for making such requests provided that:

- The request is made in writing, signed & dated by the data subject (or their legal representative).
- The data claimed to be in error or missing are clearly and unambiguously identified.
- The corrected or added data are clear and declared by the subject to be complete and accurate.

It will be explained to subjects who make a request to access their data and/or to have errors or omissions corrected, or that their data be erased, that, while their requests will be actioned as soon as is practical there may be delays where the appropriate volunteers or staff to deal with the request do not work on every normal weekday.

Where a data subject requests that their data be rectified or erased the CEO will ensure that the rectifications or erasure will be applied to all copies of the subject's personal data including those copies which are in the hands of a third party for authorised data processing.

Right of Portability

KidsAid will only provide copies of personal data to the subject (or the subject's legal representative) on written request.

KidsAid reserves the right either:

To decline requests for portable copies of the subject's personal data when such requests are unreasonable (i.e., excessively frequent) or vexatious.

To make a reasonable charge for providing the copy.

Data Retention Policy

Personal data shall not be retained for longer than:

- In the case of data held by subject consent.
- The period for which the subject consented to KidsAid holding their data.
- In the case of data held by legitimate interest of the charity.
- The period for which that legitimate interest applies. For example: in the case of data subjects who held a role, such as a volunteer, with KidsAid the retention period is that for which the charity reasonably has a legitimate interest in being able to identify that individual's role in the event of any query about it.
- In the case of data held by legal obligation.
- The period for which KidsAid is legally obliged to retain those data.

KidsAid shall regularly – not less than every 6 months – review the personal data which it holds and remove any data where retention is no longer justified. Such removal shall be made as soon as is reasonably practical, and in any case no longer than 20 working days after retention of the data was identified as no longer justified.

Privacy Impact Assessment

Trustees' Data

- The volume of personal data held for the Trustees is very low as the charity holds information of less than 10 individuals.
- The sensitivity of the data is low-moderate: the most sensitive data being DBS records, date of birth and contact details.
- The risk of data breach is small as the data are rarely used, with the majority of the data being held for a combination of legal obligation and legitimate interest.

Overall impact: Low.

Staff Data

- The volume of personal data is very low as KidsAid holds information of less than 10 individuals.
- The sensitivity of the data is low - moderate: the most sensitive data being DBS records, qualification certificates, date of birth and contact details.
- The risk of data breach is small – primarily the accidental disclosure of names and e-mail addresses.

Overall impact: Low.

Therapists Data

- The volume of personal data is low as KidsAid holds information of less than 50 individuals.
- The sensitivity of the data is moderate: the most sensitive data being DBS records, qualification certificates, insurance records, date of birth and contact details.
- The risk of data breach is small – primarily the accidental disclosure of names and e-mail addresses.

Overall impact: Low.

Volunteers Data

- The volume of personal data is very low as KidsAid holds information of less than 10 individuals.
- The sensitivity of the data is low - moderate: the most sensitive data being DBS records, date of birth and contact details.
- The risk of data breach is small – primarily the accidental disclosure of names and e-mail addresses.

Overall impact: Low.

Clients Data

- The volume of personal data is high as the charity holds information of around 2000 individuals.
- The sensitivity of the data is high: the most sensitive data being date of birth, contact information, referral documentation, assessment records and reports.
- The risk of data breach is small – primarily the accidental disclosure of names and sensitive client information.

Overall impact: High.

More information about how the charity stores, processes, secures, and disposes of clinical records and client data can be found in the Confidentiality and Privacy Policy.

Supporters' and Enquirers' Data

- The volume of personal data is moderate as KidsAid holds information of around 200 individuals or companies.
- The sensitivity of the data is low: the most sensitive data being an e-mail address and donation details.
- The risk of data breach is small – primarily the accidental disclosure of names and e-mail addresses.

Overall impact: Low.

Third Party Access to Data

Under no circumstance will KidsAid share with, sell, or otherwise make available to third parties any personal data except where it is necessary and unavoidable to do so in pursuit of its charitable objects as authorised by the CEO.

Whenever possible, data subjects will be informed in advance of the necessity to share their personal data with a third party in pursuit of the charity's objects.

Before sharing personal data with a third party KidsAid will take all reasonable steps to verify that the third party is, itself, compliant with the provisions of the GDPR and confirmed in a written contract. The contract will specify that:

- KidsAid is the owner of the data.
- The third party will hold and process all data shared with it exclusively as specified by the instructions of the Data Controller or CEO.
- The third party will not use the data for its own purposes.
- The third party will adopt prevailing industry standard best practice to ensure that the data are held securely and protected from theft, corruption, or loss.
- The third party will be responsible for the consequences of any theft, breach, corruption, or loss of KidsAid's data (including any fines or other penalties imposed by the Information Commissioner's Office) unless such theft, breach, corruption, or loss was a direct and unavoidable consequence of the third party complying with the data processing instructions of the Data Controller or CEO.
- The third party will not share the data, or the results of any analysis or other processing of the data with any other party without the explicit written permission of the Data Controller or CEO.
- The third party will securely delete all data that it holds on behalf of KidsAid once the purpose of processing the data has been accomplished.
- KidsAid does not, and will not, transfer personal data out of the UK.

Data Breach

In the event of any data breach coming to the attention of the CEO, the Information Commission's Office will immediately be informed.

If full details of the nature and consequences of the data breach are not immediately accessible the Trustees will bring that to the attention of the Information Commissioner's Office and undertake to forward the relevant information as soon as it becomes available.

Data Privacy Policy

KidsAid has a Data Privacy Policy which is available to everyone on whom it holds and processes personal data.