DATA PRIVACY POLICY

Introduction

This policy concerns KidsAid's obligations under the Data Protection Act 1998 (the Act) in relation to Trustees and all charity staff including freelance therapists and volunteers.

The purpose of the Act is to safeguard personal information. The Act covers issues such as data security, individuals' rights to access information about them and the use and disclosure of personal data. The Act applies to the personal data of an individual that is held on a computer or is held in a file by reference to specific criteria concerning that individual. It also applies to some other records such as certain medical records.

Responsibility

The Board of Trustees have delegated day to day responsibility for compliance with the Act to the CEO, who line manages the Quality Lead and they are currently the Data Controller.

All staff are responsible for complying with this policy. This policy does not, however, form part of any employee's contract of employment and may be amended at any time. If a data subject believes that KidsAid has not complied with this policy or has acted otherwise than in accordance with the Act, they should notify the Data Controller or the CEO.

Compliance with this policy will help KidsAid to meet its obligations under the Act but it does not commit KidsAid to a higher standard than is required by the Act and in some circumstances, where the Act allows, compliance with the Act will be subsidiary to other considerations.

This policy is intended to give an overview of the Act and staff obligations. Information security is the most important aspect of data protection compliance. Most of the fines under the Act relate to security breaches such as leaving an unencrypted memory stick in a public place, sending sensitive documents to the wrong recipient, disposing of confidential documents without shredding them first or accidentally uploading confidential information to the web. Further information can be found below under 'Protecting Confidentiality'.

Terminology

In this policy, KidsAid has used the terms 'personal data', 'sensitive personal data', 'data controller and processing' in the same way as they are used in the Act. Personal data means any information relating to an identified or identifiable individual.

'Identifiable' means one who can be identified directly or indirectly, by reference to an identification number or to one or more factors specific to physical, physiological, mental, economic, cultural, or social identity. It makes no difference whether someone can be identified directly from the record itself or indirectly using other information. Personal data covers both facts and opinions about an individual. KidsAid may process a wide range of personal data of trustees, staff, freelance therapists, and volunteers as part of its operation.

Personal data includes:

- Personal information that has been, or will be, word processed or stored electronically (e.g., computer databases).
- Personal information that is, or will be, kept in a file which relates to an individual or in a filing system that is organised by reference to criteria which relate to the individuals concerned (e.g., name, job title, personnel information); and
- Health records prepared by a doctor, nurse, or other health professional.

The data subject is the person the information relates to. There may be more than one data subject, such as when a record concerns an incident involving two members of staff and/or clients.

Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

The Principles

KidsAid shall comply with the data protection principles contained in the Act to help ensure that all data is:

- Fairly and lawfully processed.
- Processed for a specified lawful purpose.
- Adequate, relevant, and not excessive.
- Accurate and kept up to date.
- Not kept for longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred outside of the UK without adequate protection.

Acquiring and using Personal Data

During its operation, KidsAid may collect and process personal data. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with KidsAid by mail, phone, email or otherwise) and data we receive from referrers (for example, local authorities, schools, and families). KidsAid shall only process personal data for specific and legitimate purposes.

These include:

- Providing therapeutic interventions.
- Ensuring that KidsAid provides a safe and secure environment.
- Protecting and promoting the KidsAid's interests and objectives - this includes fundraising.
- Safeguarding and promoting the welfare of children.
- For personnel, administrative and management purposes. For example, to pay staff and to monitor their performance.
- To fulfil the KidsAid's contractual and other legal obligations.
- KidsAid's staff must not process personal data for any other purpose without the permission of the Data Controller.

When shall personal data not be used?

KidsAid shall not use personal data for any purpose that is incompatible with the purpose for which it was originally acquired without obtaining the data subject's permission.

Staff should seek advice from the Data Controller in all but the clearest of cases. If information has been obtained in confidence for one purpose, it shall not be used for any other purpose without the permission of the Data Controller.

What information should be held?

KidsAid shall not hold unnecessary personal data but shall hold sufficient information for the purpose for which it is required. KidsAid shall record that information accurately and shall take reasonable steps to keep it up to date. This includes an individual's contact and medical details.

Transfer of personal data outside the UK

KidsAid shall not transfer personal data outside the UK without the data subject's permission unless it is satisfied that the data subject's rights under the Act will be adequately protected, and the transfer has been approved by the Data Controller.

How long shall KidsAid retain personal data for?

KidsAid shall only keep personal data for as long as is reasonably necessary. More specific guidelines apply in particular situations: further details are available from the Data Controller.

Information and Explanations

Informing the data subject

If KidsAid obtains personal information from someone other than the data subject, KidsAid shall:

- Inform the data subject that KidsAid has recorded that information.
- Identify its source.
- Explain why KidsAid has acquired it, and how it will be used.
- Identify the Quality Lead as the Data Controller.
- Explain who outside of KidsAid will receive that information.

- A different approach may be necessary when medical, safeguarding and child protection or staff issues are involved; further advice is available from the Data Controller.

Explanations when asking for personal data

Unless it is already clear to the person concerned, when KidsAid asks for personal information which may be kept as personal data KidsAid shall:

- Explain which information is optional, which is mandatory, and the consequences if it is withheld.
- Explain why KidsAid is asking for that information, and how it will be used.
- Identify the Quality Lead as the Data Controller.
- Explain who outside of KidsAid will receive that information.

Protecting Confidentiality

Personal data should only be shared on a need-to-know basis. Personal data shall not be disclosed to anyone who does not have the appropriate authority to receive such information, irrespective of their seniority within KidsAid or their relationship to the data subject, unless they need to know it for a legitimate purpose.

Disclosing Personal Data outside of KidsAid

Sharing personal data with others is often permissible so long as doing so is fair and lawful under the Act. However, staff should always speak to the Data Controller if in doubt, or if staff are being asked to share personal data in a new way.

KidsAid should be careful when using photographs, videos, or other media as this is covered by the Act as well.

Information Security and Protecting Personal Data

Most of the fines under the Act relate to security breaches. KidsAid shall do all that it can to ensure that personal data is not lost or damaged, or accessed or used without proper authority, and KidsAid shall take appropriate steps to prevent these events happening. In particular:

- Paper records that include sensitive personal data shall be kept in a locked draw in a secure location.
- KidsAid uses a range of measures to protect personal data stored on computers, including file encryption, anti-virus and security software, user passwords, audit trails and backup systems.
- Staff must keep any passwords secure.
- Staff must not remove personal data from KidsAid's premises unless it is stored in an encrypted form on a password protected computer or memory device.
- Staff must not use or leave computers, memory devices or papers where there is a significant risk that they may be viewed or taken by unauthorised persons. They should not be viewed in public, and they must never be left in view in a car, where the risk of theft is greatly increased.
- Staff should be very careful when sending correspondence containing personal data (for example, email addresses should be double checked).

- Personal data must not be kept for longer than is necessary and any record containing Personal data should be securely destroyed.
- When working from home, staff must comply with all the requirements of this policy as if they were at their place of work.
- Staff must submit all company-owned devices, including laptops, tablets, smartphones, and external hard drives, before leaving the charity. KidsAid reserve the right to disable, or revoke access to all company systems, apps, cloud storage or data immediately when an employee leaves.

Rights of Access to Information and Other Statutory Rights

Data subject access request

Unless an exemption applies, individuals are entitled to know whether KidsAid is holding any personal data which relates to them, what that information is, the source of the information, how KidsAid uses it, and who it has been disclosed to.

Those wishing to access their personal data must make a subject access request in writing and KidsAid will respond within the timeframe set out in the Act (usually 40 days). To help ensure that any request is dealt with promptly, KidsAid's preference is that requests are addressed to the Data Controller.

KidsAid is entitled to charge an administration fee (usually £10) for responding to a request.

Certain data is exempt from the right of access under the Act. This may include:

- Information which identifies other individuals.
- Information which KidsAid reasonably believes is likely to cause damage or distress if disclosed.
- Data prepared solely or mainly to request or give legal advice.
- Data that does not concern a living individual.
- Data that is not part of a manual or electronic filing system.
- Data that may be evidence in criminal proceedings.

Most of the above exemptions are not absolute and their application will depend on the circumstances.

Any member of staff who receives a request for information covered by this policy from a member of staff, parent/carer or any other individual must inform the Data Controller/Quality Lead as soon as is reasonably possible, which should in most cases be the same day. This is important so that KidsAid can respond within the timeframe set out in the Act.

Data subject statutory rights

In addition to the right to make a subject access request as above, individuals have the following statutory rights:

- To ask KidsAid not to make decisions automatically (using personal data) if such automatic decisions would affect them to a significant degree.
- To ask for incorrect personal data to be corrected or annotated.

- To ask KidsAid not to use their personal data in a way that is likely to cause them unwarranted and substantial damage or distress.

Data Protection Compliance

ICO website

KidsAid has registered its use of personal data with the Information Commissioner's Office and further details of the personal data it holds, and how it is used, can be found in KidsAid's register entry on the Information Commissioner's website at www.ico.org.uk under registration number ZA011078. This website also contains further information about data protection.

Contact

If you would like any further information about anything within this policy, please contact the Data Controller.

Breach of this Policy

A member of staff who deliberately or recklessly discloses personal data held by KidsAid without proper authority may be guilty of a criminal offence and potentially gross misconduct. This may result in summary dismissal.