Data Protection Policy

1.0 Purpose

- To ensure any data collected by any means by Kids on Track is stored in compliance with the Government's General Data Protection Regulations ("GDPR" May 2018)
- To ensure such data is used, deleted or disposed of within the relevant timescale

2.0 Government Guidelines

https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation

The GDPR sets out seven key principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

"Data" is any information that could identify any individual, specifically (but not exclusively):

Personal Data	Special Data
Name	Race
Address	Religion
Email	Political affiliation
Photographs	Trade Union membership
IP address	Sexual orientation
Location	Health
Cookies	Biometric information
Profiling and analytical data	Genetic information

3.0 Current KOT Policy

All data, however received, will be:

- Processed lawfully, fairly and transparently;
- Collected only for specific legitimate purposes;
- Adequate, relevant, and limited to what is necessary;
- Accurate and up-to-date;
- Stored securely (on computers or laptops protected by a password; in locked filing cabinets);
- Only kept for as long as necessary
- Always deleted securely (by shredding paper copies of information and deleting digital information)

4.0 Collecting personal data

4.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6' lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the charity can fulfil a contract with the individual, or the individual has asked the charity to take specific steps before entering into a contract
- The data needs to be processed so that the charity can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life
- The data needs to be processed so that the charity can perform a task in the public interest, and carry out its official functions
- The data needs to be processed for the legitimate interests of the charity or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer in the case of a child) has freely given clear consent

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

4.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary. Staff must only process personal data where it is necessary in order to do their jobs. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised.

5.0 Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a child or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies. We will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings

- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of the Kids on Track children attending an event or staff or volunteers.

6.0 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the charity holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purpose of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual

Subject access requests must be submitted in writing, either by letter, email or fax to the Trustees.
They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent. Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request.

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

In addition to the right to make a subject access request and to receive information about how we use and process data, individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the Trustees.

7.0 Photographs and videos

As part of our charity activities, we may take photographs and record images of children, staff and volunteers. We will obtain written consent from parents/carers for photographs and videos to be taken of children for communication, marketing and promotional materials.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further. When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

If staff/volunteers use their own devices to take photos they will delete them from their device once they have been uploaded onto Google Drive.

See our Child Protection and Safeguarding Policy for more information on our use of photographs and videos.

8.0 Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

Data will be stored within a password protected area of Google Drive and will only be accessible by members of the committee.

9.0 Disposal of records

- Personal data that is no longer needed, has become inaccurate or out of date will also be disposed of securely. For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files.

- Once a child has left Kids on Track their data and any notes will be archived but kept on record in line with GDPR requirements in case of any future safeguarding investigations.
- Volunteer / Staff data will be deleted if we have had no contact with the individual for five years.
- The mailing list will be reviewed every two years and individuals will be asked if they wish to remain on the database.
- Supplier lists will be reviewed every two years and any inaccurate or out of date data removed.
- 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, will be disposed of in a manner which ensures that any residual personal data held on the equipment cannot be recovered by unauthorised persons.

10.0 Personal data breaches

The charity will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches may include but are not limited to:

- Names and contact details being left in a public place
- Safeguarding information being made available to an unauthorised person
- Hacking of our Google Drive
- The theft of a laptop containing non encrypted personal data about children

11.0 Privacy Statement

The Charity will have a Privacy Policy and appropriate Privacy Notices which it will make available to everyone on whom it holds and processes personal data.

In the case of data obtained directly from the data subject, the privacy notice 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 privacy notice will be provided within a reasonable period of the Charity 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.

12.0 Monitoring arrangements

The CEO is responsible for monitoring and reviewing this policy. The policy will be reviewed with Trustees every two years.

Date:	July 2020
Date for Review:	July 2021
Reviewed by:	

Data Protection Policy

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or volunteer must immediately notify the Trustees.

- The Trustees will investigate the report, and determine whether a breach has occurred. To decide, the Trustees will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been

- The Trustees will make all reasonable efforts to contain and minimise the impact of the breach

- The Trustees will assess the potential consequences, based on how serious they are, and how likely they are to happen

- The Trustees will work out whether the breach must be reported to the ICO. This must be judged on a case by case basis. To decide, the Trustees will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

- If it's likely that there will be a risk to people's rights and freedoms, the Trustees must notify the ICO.

- The Trustees will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach.

- Where the ICO must be notified, the Trustees will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the Trustees will set out:
    - A description of the nature of the personal data breach including, where possible:
        - Approximate number of individuals concerned
        - Approximate number of personal data records concerned
    - The name and contact details of the Trustees
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the Trustees expect to have further information. The Trustees will submit the remaining information as soon as possible.

- The Trustees will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the Trustees will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the Trustees
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

- The Trustees will notify any relevant third parties who can help mitigate the loss to individuals for example, the police, insurers, banks or credit card companies

- The Trustees will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing
    - more robust processes or providing further training for individuals)

We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error

- Members of staff who receive personal data sent in error must alert the sender as soon as they become aware of the error

- In any cases where the recall is unsuccessful, the sender will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way

- The Trustees will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request