SKIP Data Protection Policy

Contents

Introduction

SKIP is required to collect and store certain information (personal data) on its members (data subjects) (which includes branch volunteers, branch committee, National Committee, Trustees, Mentors and Alumni) to carry out its day to day operations, to meet its objectives and to comply with legal obligations.

SKIP is committed to ensuring any personal data will be dealt with in line with the Data Protection Act 2018 and the General Data Protection Regulation (GDPR). SKIP processes data under the category of consent; meaning personal data is freely given and the data subject has ongoing control with a positive opt in option at all times.

The aim of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures. This policy also highlights key data protection procedures within SKIP. It covers all SKIP members who are involved in the collection and processing of data.

Definitions

Personal data is information that relates to an identified or identifiable individual.

Special Category data is personal data which is more sensitive and therefore needs more protection. This may include information about an individual's

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life;
- sexual orientation.

Criminal Offence Data – refers to personal data relating to criminal convictions and offences, or related security measures.

Data subject – means an individual who is the subject of personal data

Data controller – means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed

Data processor – means any person who processes the data on behalf of the data controller

SKIP Responsibilities

Overall responsibility for personal data within SKIP rests with the Board of Trustees.

The Board of Trustees are responsible for:

- Understanding and communicating legal obligations
- Identifying potential problem areas or risks
- Producing clear and effective procedures
- Dealing promptly with any enquiries about handling personal information
- Regularly reviewing and auditing the ways SKIP manages and uses personal data

In line with legal guidances, SKIP 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
- Not held longer than necessary
- Be processed in accordance with the rights of data subjects
- Be subject to appropriate security measures
- Not be transferred outside the European Economic Area (EEA)

All SKIP members who process personal data must ensure they not only understand but also act in line with this policy and the data protection principles. Breach of this policy will result in internal disciplinary proceedings.

SKIP will ensure that:

- Everyone managing and handling personal information is trained
- Any disclosure of personal data will be in line with our procedures
- Queries about handling personal information will be dealt with swiftly and politely

Data Protection in SKIP

SKIP processes the following personal information:

- Personal contact details
- Next of kin contact details
- Past and current medical history
- Information on religious beliefs that may impact medical treatment
- Criminal record history

Personal information is kept in the following places

- Online Google-drive database
- Online secure membership database

People within the organisation who will be involved with processing personal information are:

- Branch Committee members
- National Committee members
- Trustees
- Supporting Alumni

Data Collection

Before personal information is collected, SKIP will consider the principles of data protection. SKIP will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form.

When collecting data, SKIP will ensure that the data subject:

- Clearly understands why the information is needed
- Understands what it will be used for and what the consequences are should the data subject decide not to give consent to processing
- As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed

Is aware of data retention periods

- Is, as far as reasonably practicable, competent enough to give informed consent and has given so freely without any duress
- Has received sufficient information on why their data is needed, how it will be stored, who it might be shared with and how it will be used

Informed consent is when a data subject clearly understands why their information is needed, who it will be shared with and the possible consequences of them agreeing or refusing the proposed use of the data and then gives their consent.

For special category data, such as medical history and criminal convictions, consent will be sought each time it is to be used. Special category data will not be used apart from the exact purpose for which permission was given.

Personal data collected for charity mailing lists will be consented through an opt-in system. Individuals on the mailing list are able to remove themselves from the mailing list at any time. Mailing list data will not be shared with any third parties.

Criminal Offence Data is collected through a voluntary disclosure question as well as mandatory criminal record checks due to the nature of our work with communities. The process for this is detailed in the SKIP Recruitment Policy. Data is stored securely for 3 years and only accessible to the Recruitment Co-ordinator and involved Trustees.

Data Storage

Personal data relating to SKIP members will be stored securely online and will only be accessible to relevant members of SKIP branch committees, National Committee, Trustees and Supporting Alumni.

Data which is stored nationally, is kept securely on Google-drive and an online membership database which is only accessible to members of the SKIP National Committee, Supporting Alumni and Trustees. Both systems are password protected and the passwords are changed on an annual basis.

Information will be stored for only as long as it is needed or required statute and will be disposed of appropriately. Personal data relating to branch volunteers will be reviewed annually. Criminal Offence Data will be stored for 3 years according to our Recruitment Policy; this was only be accessible to the Recruitment Co-ordinator and SKIP Trustees.

Data Disclosure

SKIP may share data with other agencies such as the local authority, funding bodies, universities, professional 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 SKIP to disclose data (including special category data) without the data subject's consent. These are:

1. Carrying out a legal duty or as authorised by the Secretary of State
2. Protecting vital interests of a Data Subject or other person
3. The Data Subject has already made the information public
4. Conducting any legal proceedings, obtaining legal advice or defending any legal rights
5. Monitoring for equal opportunities purposes – i.e. race, disability or religion
6. Providing a confidential service where the Data Subject's consent cannot be

obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill Data Subjects to provide consent signatures.

SKIP 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. SKIP intends to ensure that personal information is treated lawfully and correctly.

Data Breaches

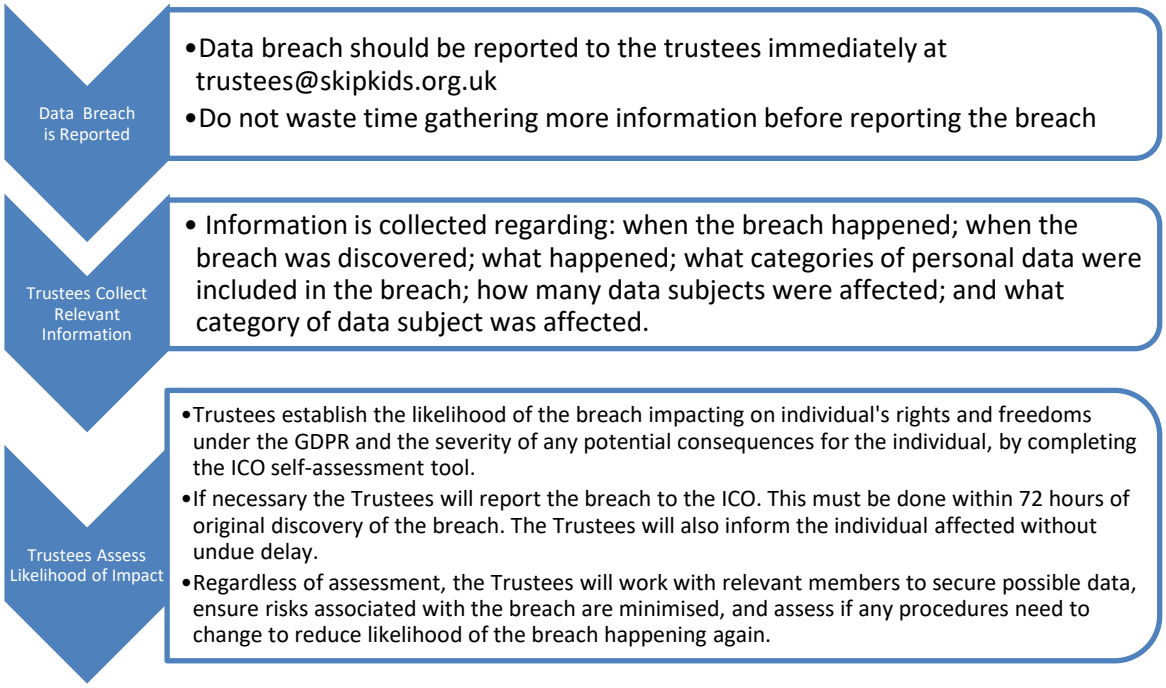
A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

Breaches can be small, relating to one person, or can affect many hundreds of individuals. A breach might involve information held in digital format or in paper files. Examples of cause might be a stolen laptop, a lost memory stick, a misdirected email, lost paperwork or unauthorised access to a system containing personal data. As well as a breach of security, data breaches can be caused in other ways, such as keeping data longer than required or gathering too much personal data.

All personal data breaches must be reported to the SKIP Trustees immediately at trustees@skipkids.org.uk

Under the GDPR, all organisations are required to report certain types of personal data breaches to the Information Commissioner's Office within 72 hours, where feasible. The Trustees will categorise the breach and make a decision about whether or not the breach should be reported to the ICO, and advise on any further actions that need to be taken (e.g. informing the individuals affected, where required).

The below flow-chart outlines the process that should be followed, should a data breach become apparent.



Where there is deliberate misconduct or behaviour amounting to a wilful breach of this Data Protection policy, or gross negligence causing a breach of the policy the matter may be considered in an internal disciplinary proceeding.

Individual Rights

As stated in the GDPR, SKIP will ensure that data subjects have the:

1. Right to be informed about the collection and use of their personal data
2. Right of access to their personal data through written request
3. Right to rectification of inaccurate personal data
4. Right to erasure i.e. to request for personal data to be deleted
5. Right to restrict processing of their personal data
6. Right to data portability i.e. obtain their own personal data
7. Right to object to the processing of their personal data in certain circumstances
8. Rights in relation to automated decision making and profiling i.e. decisions made solely by automated means without human involvement

Requests should be made by email to the SKIP Trustees who will respond within 1 month and follow legal guidance.

Data Protection Training

Training on Data Protection and how it is implemented in SKIP will take the following forms:

1. National Committee Handover Training - training session for all National Committee members and Trustees
2. Online Training – for all SKIP members

Additionally, all SKIP members will be encouraged to read the SKIP Data Protection Guide.

Policy Review

This policy will be reviewed at intervals of 3 years to ensure it remains up to date and compliant with the law. It 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 Data Protection Act 2018 and GDPR.