SCoJeC
The Scottish Council of Jewish Communities
Representing, connecting, and supporting Jewish people in Scotland

Data Processing and Protection Policy

1. ABOUT THIS DATA PROTECTION POLICY

1.1 This policy sets out how SCoJeC handles, stores, uses and shares your personal information in accordance with the **General Data Protection Regulation** (GDPR) and constitutes our Privacy Notice under these regulations.

1.2 The Scottish Council of Jewish Communities (SCoJeC) is committed to being transparent about how it collects and uses personal data and to meeting its data protection obligations. This policy sets out our commitment to the Data Protection Principles, and individual rights and obligations in relation to personal data.

1.3 This policy applies to the personal data of a number of categories of data subject, including, but not limited to:

(a) members of the Jewish Community of Scotland and others who have expressed interest in our activities by attending events, requesting information, or otherwise;

(b) individuals for whom we have submitted applications to Disclosure Scotland under the Protecting Vulnerable Groups (Scotland) Act;

(c) individuals who have reported potential crimes and other incidents to us, whether for transmission to Police Scotland or otherwise;

(d) job applicants, employees, trustees, workers, contractors, volunteers, interns, apprentices and former employees, referred to as HR-related personal data. This policy also applies to the personal data of clients or other personal data processed in pursuit of SCoJeC's charitable purposes.

1.4 SCoJeC is committed to resolving any issues about this policy as expeditiously as possible. Any questions or complains either about the policy or about our handing of your personal data should be raised as soon as possible with the Director of SCoJeC.

2. DEFINITIONS

2.1 **"Personal data"** is any information that relates to an individual who can be identified from that information. This includes the name, address, telephone number, any identification number, and anything specific to the identity of that person.

2.2 **"Processing**" is any use that is made of data, whether automated or manual, including collecting, storing, consulting, analysing, amending, transmitting, and destroying it.

2.3 **"Special categories of personal data"** means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

2.4 **"Criminal records data"** means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

2.5 The "**data controller"** is the person or persons who determine the purposes and means of the processing of personal data'.

2.6 The "**data processor**" is the person or body who processes personal data on behalf of the controller.

2.7 The "data protection principles" are:

(a) **Lawfulness, fairness and transparency**. We process personal data lawfully, fairly and in a transparent manner.

(b) **Purpose limitation**. We only collect personal data for specified, explicit and legitimate purposes and do not use it in any way that is incompatible with those purposes.

(c) **Data minimisation**. We only process personal data when it is relevant and limited to what is necessary in relation to the purposes for which it is processed.

(d) **Accuracy**. We ensure that personal data is accurate and that inaccurate personal data is corrected or deleted without delay.

(e) **Storage limitation**. We do not retain personal data for longer than is necessary for the purposes for which the data is processed, except for archiving purposes in the public interest, or for research or statistical purposes.

(f) **Integrity and confidentiality**. We have adopted procedures to ensure the security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

(g) **Accountability**. We undertake to demonstrate compliance with the regulations and general data protection principles.

3. DATA PROCESSING BY SCOJEC

3.1 SCoJeC will maintain the confidentiality, integrity, and availability of the personal data, defined as follows:

(a) Confidentiality: only people who are authorised to use the data can access it.

(b) Integrity: personal data will be accurate and suitable for the purpose for which it is processed and inaccurate personal data is rectified or deleted as soon as possible.

(c) Availability: only authorised users will be able to access the data if they need it for authorised purposes.

3.2 SCoJeC uses the names, addresses, and other contact details of its Trustees, members of Executive and Council members, in order to keep them up to date with the activities of the organisation, invite them to business meetings, etc. It is in the interests of the organisation to be able to consult its members, and we therefore believe that we have a "lawful basis for processing", namely our "legitimate Interests". We have conducted a **Legitimate Interest Assessment**, and believe that this has no impact on the individuals' privacy and tha there is no other way of achieving those those objectives.

3.3 SCoJeC uses the names and addresses (including e-mail addresses) of members of the Jewish Community of Scotland and others who have previously expressed an interest to send our mailings in order to make them aware of our activities, to solicit donations, or to other information of interest to Jewish people in Scotland. We have considered the six "lawful bases for processing" in the GDPR and believe this is in the "Legitimate Interests" both of ourselves and the recipients. We have conducted a **Legitimate Interest Assessment**, and believe this to have no impact on the individuals' privacy and to be a justified and proportionate means of achieving those objectives.

3.4 SCoJeC uses the names and e-mail addresses of individuals to circulate a number of daily or weekly bulletins of information about public affairs. We have considered the six "lawful bases for processing" in the GDPR and believe this can only be justified on the basis of the recipients' consent. We will therefore only circulate this material to those who have given their explicit consent, and will delete the details of anyone who withdraws consent as soon as possible.

3.5 SCoJeC retains the names, contact information, and Scheme Membership Number of individuals for whom we have submitted applications to Disclosure Scotland under the Protecting Vulnerable Groups (Scotland) Act in order to meet our legal obligations as a Registered Body providing a service to organisations within the Jewish Community. We do not retain the Scheme Record forms or any information about criminal records disclosed thereon beyond the three months required by Disclosure Scotland. The lawful bases for processing this information are compliance with legal obligations, protecting the vital interests of vulnerable persons, performance of a task in the public interest; and pursuing the legitimate interests of the applicant.

3.6 SCoJeC retains the names, contact details and other information provided by individuals who have reported potential crimes and other incidents to us, whether or not we have subsequently transmitted these to Police Scotland or the Community Security Trust. We do this in order to support victims of crime and monitor trends, and the lawful bases for processing this information are protecting the interests of vulnerable persons, performance of a task in the public interest; and pursuing the legitimate interests of the Jewish Community.

3.7 SCoJeC holds personal data relating to job applicants, employees, workers, contractors, trustees, volunteers, interns, and former employees, in order to be able to provide references, to demonstrate compliance with employment law, tax regulations, etc. These are held either in a locked filing cabinet or a secure password-protected electronic file. The lawful bases for processing this information

are compliance with legal obligations, and in furtherance of both our and the individual's legitimate interests.

3.8 Where SCoJeC processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with the requirements in the GDPR.

3.9 We will update personal data promptly if an individual advises that his/her information has changed or is inaccurate.

4. INDIVIDUAL RIGHTS

4.1 As data subjects, individuals have a number of rights in relation to their personal data. They can require SCoJeC to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override the organisation's legitimate grounds for processing data (where the organisation relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the organisation's legitimate grounds for processing data

4.2 As a data subject, an individual have the right to make a subject access request. If an individual makes a subject access request, SCoJeC will tell him or her:

- whether or not the data are processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- for how long the personal data are stored and for what reason;
- the individual's rights to rectification or erasure of data, or to restrict or object to processing;
- the individual's right to complain to the Information Commissioner if he or she thinks the organisation has failed to comply with his or her data protection rights.

4.3 SCoJeC will normally respond to a request within a period of one month from the date it is received. We will write to the individual within one month of receiving the original request to tell him or her if we are unable to supply the information requested within that time.

5. INDIVIDUAL RESPONSIBILITIES

5.1 Individual data subjects are responsible for helping SCoJeC keep their personal data up to date. Individuals should let us know if data provided to us changes, for example if an individual moves to a new house or changes there contact information.

5.2 Individuals may have access to the personal data of other individuals and of our contacts in the course of their employment, contract, volunteer period, internship, etc. Where this is the case, SCoJeC relies on individuals to help meet our data protection obligations.

5.3 Individuals, and in particular employees, contractors, volunteers, etc, who have access to personal data are required:

- to access only data that they have the authority of the Data Controller to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation;
- to ensure that confidential information on either their desk or their computer screen is not visible to passers-by, and that they log out of their computer when it is left unattended;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from the organisation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device.

5.4 For employees, contractors, volunteers, and other workers, failure to comply with these requirements may amount to a disciplinary offence, which will be dealt with under our Disciplinary Procedure. Significant or deliberate breaches of this policy, such as accessing data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to summary dismissal or termination of their contract.

6. DATA BREACHES

6.1 If SCoJeC discovers that there has been a breach of personal data that poses a significant risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. We will record all data breaches regardless of their effect.