RSCDS Glasgow Branch Data Protection Policy

Version 2 Last updated	16th March 2025

Definitions

Branch	means RSCDS Glasgow Branch, a registered charity (SC008002)
GDPR	means the General Data Protection Regulation.
Responsible Person	means the Glasgow Branch Committee Chair (with Chair-Elect as back-up)
Register of Systems	means a register of all systems or contexts in which personal data are processed by the Charity.

1. **Data protection principles**

The lawful bases for processing are set out in Article 6 of the UK GDPR. At least one of these must apply whenever you process personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Bullet points (a), (b) and (e) apply to the Branch. (RSCDS Glasgow Branch).

The Branch is committed to processing data in accordance with its responsibilities under the UK Data Protection Act of 2018 and UK GDPR.

Article 5 of the GDPR requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;
b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d. 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;
e. 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; and
f. 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."

2. General provisions

a. This policy applies to all personal data processed by the Branch.
b. The Responsible Person shall take responsibility for the Branch's ongoing compliance with this policy.
c. This policy shall be reviewed at least annually.

3. Lawful, fair and transparent processing

a. To ensure its processing of data is lawful, fair and transparent, the Branch shall maintain a Register of Systems.
b. The Register of Systems shall be reviewed at least annually.
c. Individuals have the right to access their personal data and any such requests made to the Branch shall be dealt with in a timely manner.

4. Lawful purposes

a. All data processed by the Branch must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests (see Information Commissioner's Office guidance for more information.)
b. The Branch shall note the appropriate lawful basis in the Register of Systems.
c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.

d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Branch's systems.

5. Data minimisation

a. The Branch shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
b. The Branch will determine who on the Branch Committee should have access to personal data and shall ensure access is appropriately limited to those individuals.

6. Accuracy

a. The Branch shall take reasonable steps to ensure personal data are accurate.
b. Where necessary for the lawful basis on which data are processed, steps shall be put in place to ensure that personal data are kept up to date.

7. Archiving / removal

a. To ensure that personal data are kept for no longer than necessary, the Branch shall put in place an archiving policy for each area in which personal data are processed and review this process annually.
b. The archiving policy shall consider what data should/must be retained, for how long, and why.

8. Security

a. The Branch shall ensure that personal data are stored securely using modern software that is kept-up-to-date.
b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
c. When personal data are deleted this should be done safely such that the data are irrecoverable.
d. Appropriate back-up and disaster recovery solutions shall be in place.

9. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Branch shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the Information Commissioner's Office.(more information on the Information Commissioner's Office website).

END OF POLICY