Policy Name: Privacy & Data Protection Policy - GDPR

Date Approved: February 2024

Review Frequency / Next Review Date: Annual / February 2025

Cooking Up is committed to protecting the personal data of clients, staff, and all stakeholders. This policy outlines the requirements for all staff, contractors, and appropriate third parties relating to the use and protection of personal data.

1. Data Protection Principles

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 charity or by its contractors and third parties ('data processors')
b. The Treasurer shall take responsibility for the charity's ongoing compliance with this policy.
c. This policy shall be reviewed at least annually.
d. As a not-for-profit organisation, the charity is exempt from registration with the Information Commissioner's Office.
e. All Cooking Up staff will be expected to be familiar with the principles of GDPR and will have completed GDPR Data Protection training on commencement of employment. Thereafter, appropriate annual refresher training will be provided.

3. Lawful, fair, and transparent processing

a. Ensure its processing of data is lawful, fair and transparent
b. Individuals have the right to access their personal data at any time and any such requests made to the charity shall be dealt with in a timely manner, with any subject access request (SAR) completed within 30 days of receipt. While most SARs will be completed at no cost, Cooking Up reserves the right to charge a reasonable fee if the administrative costs of complying with the request is manifestly unfounded or excessive, or if the request is made repeatedly.

4. Lawful purpose

a. All data processed by the charity must be done on one of the following lawful bases:

    - Consent
    - Contract
    - Legal obligation
    - Vital interests
    - Public task
    - Legitimate interests

    The majority of data processed by Cooking Up will be done on the basis of Consent e.g. workshop promotion. Any additional lawful basis for processing shall be agreed with the Treasurer.

b. The charity shall note the appropriate lawful basis in the Information Asset Register.
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 charity's systems.

5. Data Minimisation

a. The charity shall ensure that personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

6. Accuracy

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

7. Data Retention & Removal

a. To ensure that personal data is kept for no longer than necessary, the charity shall follow the following data retention guidelines (except where an alternate retention period is required by a funder or as a result of a data hold order):

Data Type	**Retention Period**
Personnel records	7 years
Recruitment data	6 months
Expense reports	7 years
Payroll information	7 years
Donor & Gift Aid data	7 years
Client sign-up sheets	1 year

b. Data retention period shall be reviewed annually as part of the annual policy review.

8. Security

a. The charity shall ensure that personal data is stored securely using modern software that is kept-up-to-date to protect against hacking, viruses, and other internet security risks.
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 is deleted this should be done safely such that the data is

irrecoverable.

d. Appropriate back-up and disaster recovery solutions shall be in place.

9. Breaches & Complaints

The charity shall have sufficient procedures in place to address potential issues arising through the processing of personal data. This includes:

- Breach – the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data
- Complaints – an expression of dissatisfaction regarding how a person's personal data has been obtained, processed, stored, or removed
- Subject Access Requests (SARs) – a request made by a data subject regarding personal data held by the charity

In the event of a breach, the charity must ensure that it promptly assesses the risk to people's rights and freedoms and if appropriate report this breach to the Information Commissioner's Office.