OASISS COMMUNITY GROUP

General Data Protection Regulation Policy v2.1

Approved by OASISS Management Committee

Date	21 November 2024
Guideline Review Date	December 2025

Data Protection Policy – v 2.1

OASISS – Open ArmS In Shelford and Stapleford

Definitions.

Community Group ….	OASISS – Open Arms In Shelford and Stapleford
GDPR….	General Data Protection Regulation Policy for OASISS
Responsible person…	A nominated person on the Committee
Register of Systems….	A register of all systems or contexts in which personal data is processed by the Community Group.

1. Data protection principles

The Community Group is committed to processing data in accordance with its responsibilities under the 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
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.
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 Community Group.
b. The Responsible Person shall take responsibility for the Community Group 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 Community Group 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 Community Group shall be dealt with in a timely manner.

4. Lawful purposes

a. All data processed by the Community Group must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task, or legitimate interests.
b. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
c. 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 Community Group's systems.

5. Data minimisation

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

6. Accuracy

a. The Community Group 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 personal data is kept up to date.

7. Archiving / Removal

a. To ensure that personal data is kept for no longer than necessary, the Community Group shall put in place archiving policy for each area in which personal data is processed, steps shall be put in place to ensure that personal data is kept up to date.
b. The archiving Policy shall consider what data should/must be retained, for how long, and why.

8. Security

a. The Community Group shall ensure that personal data is 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 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. 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 Charity shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO.

Register of Systems

MS-Excel:

Consists of computers held by Committee Members using email and a single central data base held in MS Excel by one nominated member of the same Committee.

WordPress:

The Community Group's website is created in Wordpress and is hosted by The Wordpress Foundation. Data is stored securely and never shared. The website holds the email addresses of those hosts who have subscribed to the Community Group's distribution list, by which news updates are distributed occasionally.

The Wordpress Data Privacy Policy is found here: https://en-gb.wordpress.org/about/privacy/

Google Drive:

Google forms are integrated with the website and hold limited data provided by those who use the following forms: "Offer to Host"; "Pledge Support"; "GDPR". This data is cleared from the forms annually, but retain as a record within MS-Excel, as above.

The Google Data Privacy Policy is found here:
https://support.google.com/docs/answer/10381817?hl=en

Archiving Policy

Any data held on the Community Group's Systems shall only be held for as long as needed to fulfil the purpose for which the data was intended. Thereafter it will be removed from the Community Group's systems and securely erased.

Website subscribers can request removal of their details from the Community Group's systems at any time by emailing: granta.oasiss@gmail.com

---