DATA PROTECTION

Last updated by Lucy Akrll, approved by trustees on 21/1/23

1. Data protection principles

1. Campus is committed to processing data in accordance with its responsibilities under the General Data Protection Regulation (GDPR).

2. 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

1. Campus processes personal data related to volunteers, children and young helpers, alumni, donors, parents/carers and social workers. All personal data will be treated in accordance with this policy.
2. When processing data related to children, Campus will seek parental consent as per the GDPR guidelines.
3. The Data Officer shall take responsibility for Campus' ongoing compliance with this policy.
4. Campus shall register with the Information Commissioner's Office as an organisation that processes personal data.

3. Lawful, fair and transparent processing

1. To ensure its processing of data is lawful, fair and transparent, Campus shall maintain a Register of Systems.
2. The Register of Systems shall be reviewed at least annually.
3. Individuals have the right to access their personal data and any such requests made to Campus shall be dealt with in a timely manner.
4. Where Campus processes special sensitive categories of data (for example health data), this will only be processed as part of the charitable purpose and with consent.

5. Sensitive data will be stored securely, taking into account the potential harm it could cause if disclosed.

4. Lawful purposes

1. All data processed by Campus must be done on one of the following lawful bases: consent; contract; legal obligation; vital interests; public task; or legitimate interests (see ICO guidance).
2. Campus shall note the appropriate lawful basis in the Register of Systems.
3. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
4. 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 Campus' systems.

5. Data minimisation

1. Campus shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
2. The annual review of the Register of Systems will cover which data is necessary and relevant to Campus.

6. Accuracy

1. Campus shall take reasonable steps to ensure personal data is accurate.
2. 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. Archiving and removal

1. To ensure that personal data is kept for no longer than necessary, Campus shall put in place an archiving procedure for each area in which personal data is processed and review this process annually.
2. The archiving process shall consider what data should/must be retained, for how long, and why.

8. Security

1. Campus shall ensure that personal data is stored securely using modern software that is kept up-to-date.
2. 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.
3. When personal data is deleted this should be done safely such that the data is irrecoverable.
4. Appropriate backup and disaster recovery solutions shall be in place.

9. Breach

1. 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, Campus shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO (more information on the ICO website).

Appendix

1. GDPR
2. ICO guidance
3. Register of Systems and Subject types