Data Protection Policy – GDPR

Definitions

Charity	means Slough Council for Voluntary Service, a registered charity.
GDPR	means the General Data Protection Regulation.
Responsible Person	means the Head of Operations (the Charity's Data Protection Officer)
Register of Systems	means a register of all systems or contexts in which personal data is processed by the Charity.

1. Overview

Slough Council for Voluntary Service (hereafter 'SCVS') exists to promote, enable and co-ordinate local voluntary sector action. As an employer and service provider to the community, therefore, the organisation recognises and accepts its responsibilities under the **Data Protection Act 2018** is the UK's implementation of the General **Data Protection** Regulation (**GDPR**). Everyone responsible for using personal **data** has to follow strict rules called '**data protection** principles'. They must make sure the information is: used fairly, lawfully and transparently.

2. Data protection principles

The Charity is committed to processing data in accordance with its responsibilities under the GDPR.

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

2.1 processed lawfully, fairly and in a transparent manner in relation to individuals;

2.2 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;

2.3 adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

2.4 accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay;

2.5 kept in a form which permits identification of data subjects for no longer than is necessary

for the purposes for which the personal data is 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

2.6 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.

3. General provisions

3.1. This policy applies to all personal data processed by the Charity.

3.2. The Responsible Person shall take responsibility for the Charity's ongoing compliance with this policy.

3.3. The Charity shall register with the Information Commissioner's Office as an organisation that processes personal data.

4. Lawful, fair and transparent processing

4.1. To ensure its processing of data is lawful, fair and transparent, the Charity shall maintain a Register of Systems.

4.2. The Register of Systems shall be reviewed at least annually, with each system/ project having a review.

4.3. Individuals have the right to access their personal data and any such requests made to the charity shall be dealt with in a timely manner.

5. Lawful purposes

5.1. All data processed by the charity must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests (see ICO guidance for more information).

5.2. The Charity shall note the appropriate lawful basis in the Register of Systems.

5.3. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.

5.4. 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 the Charity's systems.

6. Data minimisation

6.1. The Charity shall ensure that personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

6.2. Sensitive data (defined by the Data Protection Act 2018 as information about racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sexual life, criminal records or proceedings relating to an individual's offences) where collected by the Charity will not be kept with a person's records but will be kept separately and securely.

6.3. Equal opportunities monitoring information will be collected/stored anonymously and will only be used for reviewing how the Charity is ensuring equality of opportunity.

7. Accuracy

7.1. The Charity shall take reasonable steps to ensure personal data is accurate.

7.2. 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.

7.3. Individuals (Data subjects) have the right to ask for their personal information to be corrected if it is inaccurate or incomplete.

In addition to this, individuals may also:

- object to the Processing of their Personal data
- lodge a complaint with the Data Protection Authority (ICO)
- request erasure of their Personal data
- request restriction of Processing of their personal data.

8. Archiving / Removal

8.1. To ensure that personal data is kept for no longer than necessary, appendix 1 shows what data should/must be retained, for how long, and why.

8.2 All personal data whether in soft copy or hard copy will be marked with a date for it to be archived and removed / destroyed in line with appendix 1.

8.3. The archiving and removal of personal data is reviewed annually along with the register of systems.

9. Security

9.1. The Charity shall ensure that personal data is stored securely using modern software that is kept up-to-date.

9.2. 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.

9.3. When personal data is deleted this should be done safely such that the data is irrecoverable.

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

10. 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 (more information on the ICO website).

11. Policy Review

This policy will be reviewed by the Charity regularly and at least annually to reflect best practice in response to changes in relevant legislation or an identified failing in the policy's effectiveness.

12. SCVS Subject Data Access Requests

All individuals who are subjects of personal data held by SCVS are entitled to request access to that data at any time, including staff and volunteers. As well as access to the actual data held they also have the right to:

- know the purpose of the collection, processing, use and storage of their personal data
- know the source(s) of the Personal data, if it was not obtained from the data subject
- the recipients or categories of recipients with whom the Personal data has been shared, along with the location of those recipients
- the envisaged period of storage for the Personal data or the rationale for determining the storage period.

How to Request Access to Data:

- Should be made through the Contact Us page on the SCVS website and complete the Enquiry Form displayed on this page.
- Once received it will be logged on the central subject access log and acknowledged within three days of receipt
- Responses should be completed by the relevant manager and the Data Protection Lead must review the response is appropriate before it is sent
- A response to each Subject Access Request will be provided within 1 calendar month of it being received.
- The Subject Access Request log can be found in the Managers Folder on the One Drive.

PENINSULA

Document Retention Periods
Guidance Note

Below are two tables which show the periods for which you should keep certain pieces of information for in relation to your employees. Table 1 shows document for which the retention periods are prescribed be law. The periods shown for the documents in Table 2 are not set by law, but are recommended periods.

TABLE 1

Record	Statutory Retention Period	Authority
Accounting	Private companies – 3 years; Public limited companies – 6 years	s. 221 Companies Act 2006
Income Tax, NI returns, HMRC correspondence	3 years after the end of the financial year	The Income Tax (Employments) Regulations 1993
Children/young adults	Until the child reaches 21	Limitation Act 1980
Retirement Benefits Schemes	6 years from the end of the scheme year	The Retirement Benefits Schemes (Information Powers) Regulations 1995
Statutory Maternity Pay (calculations, certificates, medical evidence)	3 years after the end on the tax year in which the period ends	The Statutory Maternity Pay (General) Regulations 1986
Wage/salary (overtime, bonuses, expenses)	6 years	Taxes Management Act 1970
NMW	3 years after the end of the consequent pay reference period	National Minimum Wage Act 1998
Working time	2 years after they are made	The Working Time Regulations 1998

TABLE 2

Record	Recommended Retention Period
Application forms and interview notes	6 months to a year
Assessments under health and safety regulations and records of consultations with safety representatives and committees	Permanently
Inland Revenue/HMRC approvals	Permanently
Money purchase details	6 years after transfer or value taken
Parental leave	Until child is 18 (birth/adoption)
Pension scheme investment policies	12 years from the ending of any benefit payable under the policy
Pensioners' records	12 years after end of benefit
Personnel files, training records (disciplinary records, working time records)	6 years after end of employment
Redundancy details, calculations of payments, refunds, notification to the Secretary of State	6 years after date of redundancy
Statutory Sick Pay records, calculations, certificates, self-certificates	at least 3 months after the end of the period of sick leave, but 6 years after the employment ceases advisable
Time cards	2 years after audit
Trade Union agreements	10 years after end
Works Council minutes	Permanently