Data Protection Policy
Deveron Projects

Last updated: January 2024
Due for review: January 2025

The purpose and objective of this Data Protection Policy is to ensure Deveron Projects (DP) collects, processes and stores personal data in compliance with data protection laws. This policy applies to all personal data processed by Deveron Projects (note 1).

DP's other data protection policies and procedures, which relate to this policy, are:

- Record of processing activities and Data Protection Impact Assessment process
- Privacy Notice
- Personal data breach reporting process and register
- Data Retention Policy
- Cyber Security Policy

'Data Protection Law' includes the General Data Protection Regulation 2016/679, the UK Data Protection Act 2018 and all relevant EU and UK data protection legislation.

General policy with regard to Data Protection

1. It is the policy of Deveron Projects to ensure, so far as it is reasonably practicable:

    - Personal data is processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency")
    - Personal data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ("purpose limitation")
    - Personal data is accurate and, where necessary, kept up to date, and that reasonable steps will be taken to ensure that inaccurate personal data is erased or rectified without delay ("accuracy")
    - Personal data is kept in a format that permits identification of data subjects for no longer than is necessary for the purposes for which it is processed ("storage limitation")
    - Personal data is 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 and organisational measures ("integrity and confidentiality")

2. Deveron Projects will facilitate any request from a data subject who wishes to exercise their rights under data protection law as appropriate, always communicating in a concise, transparent, intelligible and easily accessible form and without undue delay.

3. The designated owner of the Data Protection Policy is DP Board of Trustees. Responsibility for maintaining and reviewing the Data Protection Policy Is delegated to DP Co-Director (Creative).

4. All staff are responsible for implementing the Data Protection Policy in their organisational areas.

5. It is the responsibility of each employee to adhere to the Data Protection Policy.

(note 1) This includes personal data belonging to our users, staff, volunteers, partners and third parties among others.

Responsibilities

Overall and final responsibility for data protection at Deveron Projects is that of the DP Board of Trustees.

Day-to-day responsibility for ensuring this policy is put into practice is delegated to DP Co-Director (Creative).

All employees have to:

- Cooperate on Data Protection matters
- Not interfere with anything provided to safeguard Data Protection
- Take reasonable care of personal data and data protection practices
- Report all personal data breaches (actual or suspected) or data protection concerns to the Co-Director (Creative).

Employees reporting risk

Data Protection Officer Is: Co-Director (Creative).

Risk Management

Deveron Projects will:

- Ensure that the legal basis for processing personal data is identified in advance and that all processing complies with the law
- Not do anything with personal data held by the organisation that would be unexpected by the data subject, given the content of this policy and DP Privacy Notice
- Ensure that appropriate Privacy Notices are in place advising data subjects how their data is being processed and advising them on their rights
- Only collect and process the personal data it needs for purposes it has identified in advance
- Ensure that there is a system in place for ensuring data is kept as up to date as possible
- Only retain personal data for as long as it is needed, after which time DP will securely erase or delete personal data. Our Data Retention Policy sets out the timeframes and conditions for data retention.

- Ensure appropriate security measures are in place to ensure personal data can only be accessed by those who need to access it, and that it is held and transferred securely.

DP will ensure that all staff who handle personal data are aware of their responsibilities under this policy and other relevant data protection and cyber security policies, and that they are adequately trained and supervised.

Intentionally breaching this policy may result in disciplinary action for misconduct, including dismissal. Obtaining (including accessing) or disclosing personal data in breach of this policy may also be a criminal offence.

Data Subject Rights

DP has processes in place to ensure it can facilitate any request made by an individual to exercise their rights under data protection law. All staff have received training and are aware of the rights of data subjects. Staff can identify such a request and know who to send it to.

All requests will be considered without undue delay and within one month of receipt as far as possible.

Subject Access: the right to request information about how personal data is being processed, including whether personal data is being processed and the right to access that data and be provided with a copy of that data along with the right to obtain the following information:

- The purpose of processing
- The categories of personal data
- The recipients of who data has been disclosed or which will be disclosed
- The retention period
- The right to lodge a complaint with the Information Commissioner's Office
- The source of any information if not collected direct from the subject
- The existence of any automated decision making

Rectification: the right to allow a data subject to rectify inaccurate personal data concerning them.

Erasure: the right to have data erased and to have confirmation of erasure, but only where:

- The data is no longer necessary in relation to the purpose for which it was collected, or
- Where consent is withdrawn, or
- Where there is no legal basis for the processing, or
- There is a legal obligation to delete data

Restriction of processing: the right to ask for certain processing to be restricted in the following circumstances:

- If the accuracy of the data is being contested, or
- If our processing is unlawful but the data subject does not want it erased, or
- If the data is no longer needed for the purpose of the processing but it is required by the data subject for the establishment, exercise or defence of legal claims, or

- If the data subject has objected to the processing, pending verification of that objection.

Data Portability: the right to receive a copy of personal data which has been provided by the data subject and which is processed in automated means in a format that will allow the individual to transfer the data to another data controller. This would apply only if SSW was processing the data using consent or on the basis of a contract.

Object to processing: the right to object to the processing of personal data relying on the legitimate interest processing condition unless SSW can demonstrate compelling legitimate grounds for the processing which override the interests of the data subject or for the establishment, exercise or defence of legal claims.

Special category data

This includes the following personal data, revealing:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data, biometric data for the purpose of uniquely identifying a natural person
- An individual's health
- A natural person's sex life or sexual orientation
- Criminal convictions or offences

DP processes special category data of users on a basis of consent. This is to provide access support, ensure their health and wellbeing while in residence and support their unique needs while working with us.

Measures are taken to ensure special category data provided by the user for the purpose of monitoring and reporting is anonymised and non-identifiable.

DP processes special category data of staff and third parties as necessary to comply with employment and social security law. This policy sets out the safeguards we believe are appropriate to ensure that we comply with the data protection principles set out above. DP also has a data retention policy which sets out how long special category data will be retained.

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, DP will promptly assess the risk to the data subject's rights and freedoms and if appropriate report this breach to the Information Commissioner's Office. This procedure is outlined in DP's Personal Data Breach Notification Procedure.

https://ico.org.uk/ [accessed 12 April 2021]