Data Protection policy – Devon and Exeter Institution

1. Introduction

This policy sets out the policy of the Devon and Exeter Institution (DEI), Registered Charity No. 1172445, regarding the data protection rights of its members and any other data subjects in respect of their personal data under EU General Data Protection Regulation (GDPR). The DEI does not need to register with the Information Commissioner's Office (ICO) as it is a not for profit organisation

1.1 Personal data

The GDPR defines personal data as 'any information relating to an identified or identifiable natural person' i.e. the data subject. An identifiable natural person is one who can be identified, directly or indirectly, by reference to a name, an identification number, location number, an online identifier or to one or more factors specific to physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

This policy defines the requirements for the collection, processing, transfer, storage and disposal of information relating to data subjects. These procedures and policies must be followed at all times by the DEI, its employees, volunteers and other parties working on behalf of the DEI.

1.2 The Data Protection principles

Lawfulness, fairness, and transparency: personal data should be processed lawfully, fairly, and in a transparent manner

Limited purpose: personal data should be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes

Data minimisation: personal data should be adequate, relevant, and limited to which it is necessary in relation to the purposes for which they are collected

Accuracy: personal data stored and managed should be accurate and, where necessary, kept up to date

Storage limitation: personal data should be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

Confidentiality and integrity: personal data should be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

1.3 The Rights of Data Subjects

- The right to be informed
- The right to access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability i.e. supplying the data to a third party if requested to do so by the data subject
- The right to object and not to be subject to automated decision-making including profiling

1.4 Data Controllers and Data Processors

DEI is the Data Controller as it controls the storage and processing of the personal data it collects

The following organisations act as Data Processors for the DEI: WebCollect; Quickbooks Online and GoCardless

1.5 Data Protection Officer

The DEI is not required to formally appoint a Data Protection Officer. However, the Board of Trustees will take responsibility for data protection compliance and will assess where a designated role sits within its structure and governance arrangements.

1.6 Data Protection Impact Assessments (DPIA)

The DEI will ensure that a DPIA is conducted before the introduction of any new technology is introduced or if there are significant changes to the collection or use of personal data

1.7 Data breaches

The DEI will notify the ICO of a breach where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

The DEI Policies are reviewed and updated annually to ensure that procedures are in place to effectively detect, report and investigate a personal data breach

1.8 Subject access requests

The DEI will respond to a request from a data subject within a period of one month

2. Lawful basis for processing

We will collect and process personal data that is relevant for recording membership of the DEI. This data may be shared with third parties that act as data processors for the DEI.

Consent will be obtained for informing members of current activities, events and consultations either by post, email or by newsletters

Our privacy policy will be published on the DEI website and a link to it provided on the online and paper membership application forms. The privacy policy will be reviewed on a regular basis.

3. Retention, migration and storage criteria for key data/information types.

Guidance from the National Archives will be sought for the retention of archival material

3.1 DEI Personal and Membership Records

Must be kept on the WebCollect membership database only. Lapsed membership records will be retained on WebCollect for no more than two years after the membership expiry date

Members' Records are available to be viewed on WebCollect by the individual member and authorised trustees or staff. These records should not normally be reproduced and held locally on personal devices nor in printed form. Various reports may be produced as required for DEI management, including an emergency contact list of trustees, staff or keyholders, but a record of where they are held and for how long must be retained.

3.2 Application Forms

Hard copies of all application forms and signed copies of the 'Expectations of our members' leaflet should be shredded as soon as the information is entered on WebCollect.

3.3 Personal Training Records
Records may be held locally for the duration of a member's or volunteer's term with DEI and retained for a maximum of one years after a volunteer leaves.

3.4 Rosters
These should be retained for a maximum of three months only. Consideration should be given to replacing paper-based records with an electronic diary such as Office 365 Online which can provide a link to everyone needing to see them.

3.5 Contact names for social events/ talks /outings etc
Paper records of these should be shredded immediately after the event or after information had been transferred to data processing records e.g. QuickBooks Online, WebCollect

3.6 Library loan records
These should be retained for a maximum of three months after the loan is returned.

3.7 Minutes of meetings
Board of Trustee and Committee minutes and papers should be retained on Office 365 permanently as part of the DEI historical record. Paper copies will be retained according to National Archive guidelines

3.8 Working papers and correspondence
Judgement should be made by trustees on retention of these documents but generally a maximum of three years, unless they form part of an ongoing activity e.g. confirmation of a legacy, or will contribute to the DEI's historical record

Retained documents should be stored on Office 365 Online wherever possible. Any paper documents no longer required should be shredded or burnt and those retained should be stored securely under lock and key.

3.9 Emails and attachments
These should be retained for a maximum of one year unless they are deemed important (e.g. contracts/personnel issues) in which case they should be filed with the relevant documentation.

All DEI trustees and staff involved in the management of the Charity will be allocated *@devonandexeterinstitution.org* email addresses (which will also be their login usernames for Office 365 Online). Emails currently stored on personal devices which need to be kept will need to be migrated to Outlook within Office 365 Online.

3.10 Financial and Management information
These should be retained for six complete years together with the year in progress. This includes Accounts, Gift Aid claims, and Expense claims. It also includes any supporting documentation pertaining to these records.

Ownership of these records normally lies with the DEI Treasurer; however other staff and/or trustee will require access. Under GDPR these records should no longer be stored permanently on personal devices or in personal online storage such as Dropbox or Googledrives. The file sharing facilities of Office 365 Online or alternatives provide a practical solution.

3.11 Contracts and Associated documents
These should be retained for the period of the contract and seven years thereafter. These documents should be securely stored under lock and key. If this is not possible, they should be scanned and uploaded to Office 365 Online as appropriate.

3.12 Newsletter
This should be retained indefinitely on Office 365, as part of our historical record.

3.13 Consultations and Evaluations
Personal information will be analysed in a non-identifiable form and no personal records will be retained.

3.14 Asset Registers
These should be maintained and up to date and eventually migrated to Office 365 Online

3.15 Website and social media presence
Cookies will not be used on the DEI website and no personal information published on any other social media. Prior individual permissions will be sought before publishing personal photographs.

3.16 Hard copy storage
Paper documents are considered the least secure form of information storage by GDPR guidance. Therefore, it is recommended that as little paper is kept as possible. Paper documents that are required should be stored appropriately according to their sensitivity and within DEI policies and Procedures. Documents required for day to day reference, such as the current roster and telephone contact lists should be stored in ready use files rather than on public display. Paper documents which are no longer required should be disposed of by shredding or burning. Reducing paper files will also alleviate the chronic storage limitations within the DEI.

3.17 Working on Personal Devices
There will be times when it is necessary to keep documents on personal devices to work on them, but the aim should be to keep such storage to a minimum. Files will be stored on a secure cloud-based system such as Office 365 online

25. Children
Consent from parents/ guardians/ carers is obtained before recording personal information. Our Safefeguarding Policy has been updated.

27. IT solutions
GDPR compliance requires the use of Office 365 Online or similar system to provide secure, shared storage. The use of Dropbox for transmitting photographs is recommended and systems appropriate to the needs of the DEI are being installed to provide cost effective solutions. User training is being delivered

28. All means of paper and electronic data capture need revision to ensure that they reflect this data protection policy, including obtaining appropriate consents, and reprints or revisions or removal requests for information introduced where necessary. This will include:

- Membership application details on paper form and WebCollect
- Publicity flyers, pamphlets and packs

29. Review of this policy
This policy is kept under review and we reserve the right to change this at any time.

May 2018