Devon Mind Data Protection Policy & Procedure

Last reviewed by Quality & Standards Committee	November 2022
Last reviewed by legal specialists (Tozers LLP)	February 2023
Ratified by Devon Mind Board of Trustees	April 2023
Review cycle	Every two years
Next review due	April 2025
Owner	Chief Executive

www.devonmind.com

Registered charity no. 1181767

Registered company no. 10281020

1. Introduction

1.1 Devon Mind is committed to compliance with all national UK laws in respect of personal data, and to protecting the rights and privacy of individuals whose information the organisation collects in accordance with the UK General Data Protection Regulation (GDPR) and the UK laws that implement it (Data Protection Act 2018).

1.2 The purpose of data protection legislation is to protect the rights and privacy of living individuals, and to ensure that personal data is not processed without their knowledge.

1.3 This Data Protection Policy is designed to ensure that Devon Mind complies fully with data protection legislation and that personal data is fairly, lawfully, and transparently processed.

1.4 Devon Mind has a dedicated Data Privacy Officer (DPO) who is responsible for overseeing this Data Protection Policy. The DPO can be reached:

- via post to Data Privacy Officer, Devon Mind, Guild House, 156 Mannamead Road, Plymouth PL3 5QL,
- via email to admin@devonmind.com, and
- via telephone on 01752 512 280.

Please contact the DPO with any questions about the operation of this Data Protection Policy or the UK GDPR or if you have any concerns that this Data Protection Policy is not being or has not been followed.

1.5 Devon Mind is registered with the Information Commissioner's Office, ICO number ZA508665.

2. Scope of this policy

2.1 Data protection legislation applies to all personal data throughout its lifespan, from the point of collection to its eventual destruction. Personal data includes any piece of information which enables the identification of a living individual, such as a name, contact details, or health information. For the purposes of this policy, references to personal data shall include special category (i.e., sensitive) personal data, unless stated otherwise.

2.2 The format in which the information is held is in most instances not relevant. If personal data exists in any form, whether electronic or in a paper-based filing system, it is covered by data protection legislation.

2.3 This policy applies to all staff and volunteers of the organisation and third-party contractors. You should familiarise yourself with this policy, the Confidentiality Policy, and Devon Mind's other information policies, and comply with their terms when processing personal data on our behalf.

3. Purpose and aims of this policy

3.1 To protect the rights and privacy of living individuals who access Devon Mind services, work for, or support Devon Mind.

3.2 To ensure that personal data is not used, stored, or disclosed ('processed') without such individual's knowledge, and is processed with a lawful basis and in a fair and transparent manner.

4. Policy statement

4.1 Devon Mind is registered with the ICO to process certain information

about staff, volunteers, third-party contractors, clients, and supporters to provide the following:

- mental health support services,
- fundraising, campaigning, and membership services,
- monitoring, evaluation, and audit of service provision, and
- training.

4.2 When processing personal data, we must comply with the six principles of good practice identified in Article 5 of the GDPR. They say that personal data shall be:

1. processed lawfully, fairly, and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'),
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, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation'),
3. adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'),
4. 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 ('accuracy'),
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 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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation'), and

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 ('integrity and confidentiality').

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above ('accountability').

4.3 In simple terms, this means we must collect and use personal data lawfully and fairly, tell people how we will use their personal data, store it safely and securely, and not disclose it unlawfully to third parties. We need to be careful that the information we collect is relevant and that we do not collect more information than we need for the stated purpose.

4.4 Information should not be transferred outside of the UK unless it meets the requirements of data protection legislation. Any such transfers require approval from the DPO.

4.5 Partners and any third parties working with or for the organisation, and who have or may have access to personal data, will be expected to comply with the principles of this policy. No third party may access personal data held by the organisation without having first entered into a third-party agreement which imposes on the third-party obligations no less onerous

than those to which the organisation is committed, and which gives the organisation the right to audit compliance with the agreement.

5. Data collection

5.1 There are multiple teams at Devon Mind who collect and process personal data. Many of these teams have different rules relating to what they do with the data. Staff should not contravene any of these rules. If you are unsure, please contact the DPO.

5.2 Data minimisation is important to think about prior to the collection of any personal data and we should only collect information that is absolutely necessary.

5.3 Data owners must ensure that they have a lawful basis for processing personal data. Under the UK GDPR, there are six lawful bases for processing non-sensitive personal data as follows:

1. **Consent**: the individual has given clear consent for you to process their personal data for a specific purpose,
2. **Contract**: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract,
3. **Legal obligation**: the processing is necessary for you to comply with the law (not including contractual obligations),
4. **Vital interests**: the processing is necessary to protect someone's life,
5. **Public task**: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law, and

6. **Legitimate interests**: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. This cannot apply if you are a public authority processing data to perform your official tasks.

5.4 Stricter rules apply to special category (sensitive) personal data, such as information about a person's health, ethnic origin, or religious beliefs, as well as information about criminal offences. We can only collect this information under very limited circumstances – for example, the person has given explicit consent, or it is necessary for specific reasons permitted by law. If in doubt, please contact the DPO.

6. How does this affect me?

6.1 Devon Mind could be fined or could face a claim for compensation if you use or disclose information about other people without their consent or reliance on other lawful grounds. To help keep personal data secure, you should take particular care when using the Internet, e-mail, and the internal network, or talking on mobile or landline telephones. You could be committing an offence if you steal or recklessly misuse personal data.

6.2 Special care must be taken with special category (sensitive) personal data, such as information relating to race, ethnic origin, religious/political beliefs, health data, disabilities, sexual life, genetics, biometrics, or trade union membership. Details of criminal offences or alleged offences must also be handled with special care.

6.3 Any breach of data protection legislation or this policy will be dealt with under Devon Mind's disciplinary policy and may also be a criminal offence, in

which case the matter will be reported as soon as possible to the appropriate authorities.

7. Responsibilities under data protection legislation

7.1 Devon Mind is a data controller under data protection legislation.

7.2 The Senior Management Team and all those in managerial or supervisory roles throughout Devon Mind are responsible for developing and encouraging good information handling practices within the organisation. The DPO has direct responsibility for ensuring that the organisation complies with data protection legislation, as do line managers in respect of data processing that takes place within their area of responsibility.

7.3 The DPO has specific responsibilities in respect of procedures such as the subject access request (SAR) procedure and is the first point of call for staff seeking clarification on any aspect of Devon Mind's data protection compliance.

7.4 Compliance with data protection legislation is the responsibility of all members of Devon Mind who process personal data.

7.5 Members of the organisation are responsible for ensuring that any personal data supplied by them, and that is about them, to Devon Mind is accurate and up to date.

8. Individuals' rights

8.1 Individuals have the following rights regarding data processing and the data that is recorded about them:

- the right to be informed about how we process their personal data,
- the right to access their personal data,
- the right to rectify their personal data,
- the right to have their personal data erased,
- the right to restrict processing of their personal data,
- the right to have a copy of their personal data in a portable form,
- the right to object to direct marketing and profiling, and
- rights in relation to automated decision making and profiling.

8.2 Where a person requests access to their information, this is called a subject access request (SAR). If you receive a request, you should forward it on to the DPO immediately. Devon Mind must adhere to the following:

- the SAR must be responded to within one month (this can be extended for a further two months if the request is complex or if a number of requests have been received from an individual),
- the response must be in a permanent form, unless this is not possible or the individual agrees otherwise,
- unintelligible terms must be explained, and
- the data must not be changed between receipt of a SAR and sending the information to the applicant, except for routine amendment of the data which would happen in any case. Care should be taken though if data relating to third parties is included.

8.3 There are some exemptions to the rights detailed above, the details of which are included in the SAR procedure – please refer to the **Devon Mind Access to Information Policy** for this.

9. Consent and transparency

9.1 Personal data should not be obtained, held, used, or disclosed unless the individual has given consent or there is another lawful basis that allows us to do so. The organisation understands "consent" to mean that the data subject has been fully informed of the intended processing and has signified (by an affirmative action) their freely given agreement, preferably in writing, whilst being in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or based on misleading information will not be a valid basis for processing. See the **Devon Mind Data Consent Policy** for further information.

9.2 All Devon Mind services should display or make available adequate privacy notices to clients and service users explaining how Devon Mind processes their information. We must provide privacy notices even if we do not need to ask for consent.

10. Security of data

10.1 All staff are responsible for ensuring that any personal data which the organisation holds and for which they are responsible is kept securely and is not disclosed to any third party, unless that third party has been specifically authorised by the organisation to receive that information and has entered into a confidentiality agreement.

10.2 You must not remove personal data from Devon Mind's premises either in electronic or paper form unless it is absolutely necessary – for example, in cases where staff have to attend external meetings, etc. Data should not be removed from the premises in a paper format unless there is no reasonable alternative. If data is in a paper format, the staff member

handling such data should ensure that any names of people and/or any information that could lead to identification of subject individuals is transported and stored securely.

10.3 Personal data pertaining to supporters or beneficiaries should be stored securely on Devon Mind systems and not be taken out of the office in paper or electronic format at any time unless a risk assessment has been undertaken and this is approved by the DPO.

10.4 Two-factor authentication must be used on all electronic devices and passwords are not to be auto-saved for systems on which personal data is stored.

10.5 Staff must comply with the information handling requirements in **Devon Mind's Confidentiality Policy**.

11. Disclosure of data

11.1 Devon Mind must ensure that personal data is not disclosed to unauthorised third parties, which includes family members, friends, government bodies, and in certain circumstances, the police. All staff should exercise caution when asked to disclose personal data held on another individual to a third party.

11.2 All third-party requests to provide data must be supported by appropriate paperwork and specifically authorised by the DPO.

12. Retention and disposal of data

12.1 Personal data may not be retained for longer than it is required – for

example, after a member of staff has left the organisation, it may not be necessary to retain all the information held on them. Some data will need to be kept for longer periods than others. Devon Mind's retention and data disposal procedures will apply in all cases.

12.2 Personal data must be disposed of in a way that protects the rights and privacy of data subjects (for example, shredding, disposal as confidential waste, secure electronic deletion) and in line with the **Devon Mind Record Retention & Disposal Policy & Procedure**.

12.3 Personal data may need to be kept for a certain period under other legislation such as accounting or tax laws. In such cases, reasonable measures must be taken to ensure it is kept securely in accordance with industry standards.

12.4 Duplicate copies of personal data should not be kept, as doing so increases the risk of that data being compromised. Where there is a need to have two copies of personal data for a short timeframe to complete a task, one copy should be deleted as soon as it is no longer needed.

12.5 All information pertaining to staff, volunteers, and trustees is to be held on the secure HR system Breathe. All documents are to be scanned and saved on the system and paper copies destroyed securely.

13. Data protection by design

13.1 Personal data must be protected, and data protection legislation requires data protection to be taken into account whenever a new system or process is introduced, or where a system or process is changed that involves processing personal data.

13.2 Data protection impact assessments (DPIAs) must be completed and approved by the DPO for any significant changes to how personal data is processed at Devon Mind that are likely to result in a high risk to individuals and where any new technologies or systems are used. A DPIA is required if:

- installing a new CCTV system,
- carrying out automated decision-making where it may have a legal or similarly significant effect on an individual, and
- carrying out a project involving large-scale processing of sensitive data or information relating to criminal convictions.

14. Working with third party partner organisations

14.1 All Devon Mind projects funded in partnership with other third party organisations should include, within the contractual agreement, a clear statement as to the extent to which Devon Mind and the third party partner organisation is responsible for compliance with data protection legislation (as data controller and/or data processor) and the respective obligations of Devon Mind and the third party partner organisation with regard to data protection. For example, where Devon Mind shares personal data with a third party provider, such as where an external provider is used for training, there must be a contract setting out that Devon Mind is the data controller and the third party is a data processor, and the respective obligations of both parties under data protection legislation.

14.2 All new contracts with third party partners or providers with whom we are sharing personal data need to be authorised by the DPO.

14.3 In addition, any external parties such as contractors with access to personal data during the course of their work will be required to conform to Devon Mind confidentiality standards and this policy and must demonstrate their agreement in writing.

15. Personal data breaches

15.1 The **Information Breach Policy** provides details about the steps that need to be taken when a personal information breach occurs – for example, loss of a memory stick or accidental disclosure of personal data to a third party. Where the breach is likely to result in a risk to individuals, the DPO must notify the ICO at the soonest possible time and within 72 hours of Devon Mind becoming aware of the breach. If the risk of the breach is high, the individuals who are affected must be informed directly and without undue delay.

15.2 You should report all breaches to your manager, IT, and the DPO who will decide how to respond to the breach and whether it needs to be notified – see the Information Breach Policy for more information.

16. Anonymisation

16.1 Anonymisation is the process of removing information that could lead to an individual being identified (for example, names and other obvious identities which reveal the identity of the individual). Personal data should be anonymised whenever it is practical and appropriate to do so. Anonymising personal data significantly reduces the risks to individuals if that information is compromised.

16.2 Where personal data is collected and needs to be retained for statistical purposes, but it no longer needs to be attributable to an individual, it should be anonymised at the earliest opportunity.

16.3 Fully anonymised data can be difficult to achieve in some situations due to the nature or context of the data, or the purpose for which it is collected, used, and retained. Where this is the case, it is still good practice to partially anonymise the data to lower the chance of it identifying an individual.

17. Roles and responsibilities

17.1 **Senior management and the Board of Trustees**: Overall responsibility for compliance with data protection legislation rests with the CEO. The CEO is responsible for making sure that the data protection function is fully resourced to meet the needs of Devon Mind. The Board of Trustees are responsible for monitoring and reviewing all data protection policies and procedures, with input from senior management.

17.2 **The Data Privacy Officer**: Operational adherence to this policy is delegated to the DPO, who is responsible for:

- understanding and communicating obligations under data protection legislation,
- identifying potential problem areas or risks,
- producing effective procedures, and
- notifying and annually reviewing notification to the ICO.

17.3 **Managers and heads of departments** are responsible for promoting data protection awareness and compliance with data protection legislation and

this policy within their teams. This includes working with the DPO to respond to data SARs from members of the public or staff. Managers and heads of departments are also responsible for making sure that all staff in their teams have been accorded the necessary data protection training. Managers must ensure that all new staff take the mandatory data protection training and review this policy as part of their induction.

17.4 **All staff, volunteers, and trustees** must ensure they understand and act in accordance with this policy and data protection legislation. Staff, volunteers, and trustees should also ensure that they keep the DPO updated if they become aware of any proposed changes or changes to the ways in which personal data is being processed by their team.

17.5 Staff, volunteers, or trustees found to be acting contrary to this policy may be subject to disciplinary action. This is because any breach of data protection legislation could result in Devon Mind facing legal action.

18. Monitoring, audit, and review

18.1 The Board of Trustees is responsible for managing this policy and overseeing its implementation. The CEO is responsible for implementing the policy within their areas of work, and for overseeing adherence by staff and volunteers. Every member of staff and volunteer should take personal responsibility for conforming to it.

18.2 It is the responsibility of the CEO to audit compliance with all policies as part of the charity's normal audit cycle and to undertake or direct remedial action as required.

19. Associated policies and procedures

Access to Information Policy & Procedure

Confidentiality Policy & Procedure

Consent Policy & Procedure

Data Retention and Disposal Policy & Procedure

Information Breach Policy & Procedure

Information Security Policy & Procedure

Information Sharing Policy & Procedure

Privacy Policy