Oxfordshire Mind

Data Protection and Confidentiality Policy

October 2023

Oxfordshire Mind
2 Kings Meadow
Osney Mead
Oxford
OX2 0DP
Tel: 01865 263730
Fax: 01865 263732

office@oxfordshiremind.org.uk
www.oxfordshiremind.org.uk

Registered Charity Number 261476
Company Limited by Guarantee 434362

Policy Owner	Chief Executive Officer
Policy Author	Head of Innovation
Document status and version number	approved

Policy(ies) which this policy would replace	Data Protection & Confidentiality Policy – final approved – March 2023
Key changes from previous version	The new policy: - Changes the designation of 'Data Protection Officer' to 'Data Protection Lead' in order to give more flexibility about how the role is placed within the organisation; and - Removes procedural guidance from the policy to facilitate more agile review and development.
Policies to which this policy cross-refers	Child Protection and Safeguarding Policy Safeguarding Adults Policy Responsible Employment Policy (Volunteer Code of Conduct)
Reference sources	https://ico.org.uk/ https://connectingminds.org.uk/resources/policy-checklist-data-protection-policy/

Contents

1. Context and purpose

1.1 Oxfordshire Mind ('the charity') 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 data protection legislation, i.e. the General Data Protection Regulations (GDPR) and the UK laws that implement it (Data Protection Act 2018).

1.2 The purpose of the 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 Oxfordshire Mind is registered with the Information Commissioner's Office as both data controller and data processor under the Data Protection Legislation.

2. Scope

2.1 This policy covers all personal data, including physical and digital data, special category and/or criminal offence data, and information from all data subjects (including staff and volunteers).

2.2 This policy applies to everyone involved in providing services at Oxfordshire Mind across its various locations ('all workers'). For the avoidance of doubt, this includes full-time employees, part-time employees, contractors and sessional workers, consultants, secondees, locums, students on placement, trustees and volunteers. Oxfordshire Mind uses the trading name 'Mind in Berkshire' for some of its Berkshire activities, but Mind in Berkshire is not a separate legal entity. Oxfordshire Mind policies therefore apply to everyone from Oxfordshire Mind involved in providing services in Berkshire, although they may be held out as 'Mind in Berkshire workers'.

2.3 Employees should also refer to the Responsible Employment Policy, and volunteers should also refer to the Volunteer Code of Conduct. There are separate confidentiality agreements for volunteers including trustees and third-party contractors such as cleaners and freelancers. Staff have a confidentiality clause included in their contract of employment.

3. Roles and Responsibilities

Trustees

3.1 Trustees retain ultimate responsibility for data protection and confidentiality. They ensure systems are fit for purpose through regular reporting and internal spot-checks/audits.

Senior Management

3.2 Overall responsibility for compliance with data protection legislation rests with the Chief Executive Officer (CEO). The CEO is the Senior Information Risk Officer (SIRO) responsible for making sure that the data protection function is properly resourced to meet the needs of the charity.

Data Protection Lead

3.3 Oxfordshire Mind has appointed Data Protection Leads (DPLs), who can be contacted on: dataprotection@oxfordshiremind.org.uk

3.4 The DPLs are responsible for the operationalisation of this policy, including:
being first point of contact for data breaches, data breach recording and follow up
processing subject access requests, understanding and communicating obligations under the data protection legislation, ensuring privacy notices are in place and up to date for staff, volunteers, and service users, identifying potential problem areas or risks

producing and monitoring effective procedures, ensuring high levels of awareness amongst staff of their responsibilities via various routes i.e., communications, training, and posters.

Managers and Heads of Departments

3.5 Managers and Heads of Departments are responsible for promoting data protection awareness and compliance with data protection legislation and this policy within their teams, including appointment and training of an Information Asset Owner if the team is collecting, processing, or storing personal data.

3.6 Managers must ensure that all new staff undertake the mandatory data protection training and understand this policy as part of their induction.

Information Asset Owners (IAO)

3.7 There are several teams at Oxfordshire Mind which collect and process personal data. Each team collecting data is required to have an appointed Information Asset Owner (IAO) who ensures and documents:

- The lawful basis for collection and processing data and, if via consent, how this is secured
- The appropriate Retention Period for this data
- The Deletion process used for this data
- How Data Minimisation principles are upheld

IAOs are responsible for ensuring up to date entries are maintained in the organisational Information Asset Register (IAR) for the data they oversee in this way.

All Staff, Volunteers and Trustees

3.8 It is the responsibility of all staff, volunteers, and trustees to ensure they understand and act in accordance with this policy and data protection legislation.

3.9 Staff, volunteers, and trustees should also ensure that they keep the Data Protection Lead(s) updated if they become aware of any proposed changes or changes to the ways in which personal data is being processed by their team.

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

4. Training

4.1 The organisation is responsible for ensuring that workers receive appropriate training on data protection to enable them to fulfil their responsibilities and obligations under the GDPR and the Data Protection Act 2018. All workers who handle personal data must receive training on data protection. This should cover the following topics:

- The principles of data protection, including the legal basis for processing personal data, the data subject's rights, and the organisation's responsibilities.
- The organisation's data protection policy and procedures, including the procedures for responding to subject access requests and data breaches.
- The technical and organisational measures that the organisation has implemented to protect personal data, including access controls, encryption, and data minimisation.
- The potential risks to personal data and how to mitigate these risks.

- The consequences of non-compliance with data protection regulations, including the penalties for breaches and the potential impact on the organisation's reputation.

4.2 The organisation will provide training through the following methods:

- Induction training for new starters, which should include an overview of the organisation's data protection policy and procedures.
- Ongoing training for all workers on an annual basis or as necessary, which should cover knowledge refreshes, updates to the organisation's data protection policy and procedures, and well as any new risks or threats to personal data which have been identified.
- Specialised training for workers who handle particularly sensitive or high-risk personal data, which should cover additional measures to protect the data and how to respond to incidents or breaches - for example:
    - Finance workers
    - HR workers
    - Data Protection Leads
    - Anyone processing special category data, e.g. health data

4.3 The organisation will evaluate the effectiveness of its data protection training programme on an ongoing basis by assessing the level of compliance with data protection regulations, the number of data breaches and incidents, and the feedback from employees, contractors, and volunteers.

4.4 The organisation will review and update this policy on an annual basis to ensure that it remains up-to-date and in compliance with applicable data protection regulations.

5. Compliance with GDPR principles

5.1 When processing personal data in the context of work with Oxfordshire Mind, all workers must comply with the six principles of good practice identified in Article 5 of the GDPR.

1) Lawfulness, fairness, and transparency: Personal data must be processed lawfully, fairly, and in a transparent manner. This means that individuals must be informed about the processing of their personal data, and the processing must be done in accordance with applicable data protection laws and regulations.

2) Purpose limitation: Personal data must be collected for specified, explicit, and legitimate purposes, and not further processed in a way that is incompatible with those purposes. This means that organisations must be transparent about why they are collecting personal data and must not use it for purposes other than those for which it was collected.

3) Data minimisation: Personal data must be adequate, relevant, and limited to what is necessary for the purposes for which it is processed. This means that organisations should only collect and process the minimum amount of personal data necessary to achieve the processing purpose.

4) Accuracy: Personal data must be accurate and kept up to date, with appropriate measures taken to ensure that inaccurate or incomplete data is corrected or erased. This means that organisations must take reasonable steps to ensure that the personal data they process is accurate, complete, and up-to-date.

5) Storage limitation: Personal data must be kept in a form that allows identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. This means that organisations must establish and adhere to specific retention periods for different types of personal data.

6) Integrity and confidentiality: Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing, accidental loss, destruction, or damage. This means that organisations must take appropriate technical and organisational measures to ensure that personal data is protected against unauthorised access, disclosure, or destruction.

In simple terms, this means the charity must collect and use personal data fairly, tell people how it will use their personal data, store it safely and securely and not disclose it unlawfully to third parties. The charity needs to be careful that the information it collects is relevant and that it does not collect more information than needed for its stated purpose.

5.2 There are restrictions on the transfer of personal data outside the European Economic Area (EEA) and information should not be transferred outside of the UK unless it meets the requirements of current data protection legislation. Any such transfers require a Data Protection Impact Assessment and approval from a Data Protection Lead and the CEO as SIRO.

5.3 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.

6. Lawful basis (principle 1)

6.1 A lawful basis for collecting, processing, and storing personal must be identified and recorded in the Information Asset Register.

Non-sensitive personal data
6.2 Under the General Data Protection Regulations (GDPR), non-sensitive data includes all data that isn't listed in special category/ sensitive data below. Examples of non-sensitive data include contact details, NI numbers and bank details.
The legal bases that can be used for this data are.

- Consent*
- Necessary as part of a contract
- Comply with a legal obligation
- Protect the vital interests of an individual
- Fulfil a public task
- Part of the organisation's legitimate interests (provided the latter is balanced against the rights of the individual).

*Because consent can be removed at any time Oxfordshire Mind's preference is not to use consent wherever possible. The legal basis for legitimate interest assessment tool should be used to ensure legal compliance.

Special category/sensitive data
6.3 Stricter rules apply to special category data which is defined as data relating to.

- Health
- Ethnicity
- Religious beliefs
- Trade Union membership
- Sexual orientation

- Criminal offences

6.4 For special category/sensitive data the organisation can only collect, process, or store this information in the circumstances/on the legal bases set out in Article 9 of GDPR which are.

(a) Explicit consent*

(b) Employment, social security, and social protection (if authorised by law)

(c) Vital interests

(d) Not-for-profit bodies

(e) Made public by the data subject

(f) Legal claims or judicial acts

(g) Reasons of substantial public interest - subject to exemption conditions listed below

(h) Health or social care (with a basis in law)

(i) Public health (with a basis in law)

(j) Archiving, research and statistics (with a basis in law)

6.5 If using g) Reasons of substantial public interest (with a basis in law) the organisation must meet at least one of the 23 exemption conditions below

- Statutory and government purposes
- Administration of justice and parliamentary purposes
- Equality of opportunity or treatment
- Racial and ethnic diversity at senior levels
- Preventing or detecting unlawful acts
- Protecting the public
- Regulatory requirements
- Journalism, academia, art, and literature
- Preventing fraud
- Suspicion of terrorist financing or money laundering
- Support for individuals with a particular disability or medical condition
- Counselling
- Safeguarding of children and individuals at risk
- Safeguarding of economic well-being of certain individuals
- Insurance
- Occupational pensions
- Political parties
- Elected representatives responding to requests
- Disclosure to elected representatives
- Informing elected representatives about prisoners
- Publication of legal judgments

- Anti-doping in sport
- Standards of behaviour in sport

Type of data, non-sensitive/sensitive, and legal basis must be recorded and regularly updated for each relevant team on the Information Asset Register.

7. Individuals' Rights

7.1 Individuals have the following rights regarding data processing, and the data that is recorded about them, to:

- Be informed about how we process their personal data
- Access their personal data
- Rectify their personal data
- Have their personal data erased
- Restrict processing
- Have a copy of their personal data in a portable form
- Object to direct to marketing and profiling
- Rights in relation to automated decision making and profiling.

7.2 Where a person makes any of the eight requests above, this is called a data Subject Access Request ('SAR'). SARs must be acknowledged promptly and the DPL notified at dataprotection@oxfordshiremind.org.uk in accordance with the organisation's SAR procedure.

7.3 Oxfordshire Mind locations should display or make available adequate notices to service users explaining how the charity uses and processes their information.

7.4 Staff and volunteers will be required to sign separate privacy notices during their starting process.

8. Security of Data

8.1 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.

9. Disclosure of Data

9.1 Oxfordshire 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. Data shared must be minimal, accurate and proportional.

9.2 All third-party requests to provide data must be supported by a Subject Access Request form and specifically authorised by the Data Protection Lead.

10. Retention & Disposal of Data

10.1 Personal data may not be retained for longer than it is required. Some data will need to be kept for longer periods than others. Oxfordshire Mind's retention and data disposal procedures will apply in all cases.

10.2 Personal data must be disposed of in a way that protects the rights and privacy of data subjects (e.g., shredding, disposal as confidential waste, secure electronic deletion) and in line with Oxfordshire Mind's Record Retention Procedure contained within the Information Asset Register.

10.3 Personal data may need to be kept for a certain period of time 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.

11. Changes to or new systems/processes (DPIA)

11.1 Personal Data must be protected, and the 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.

11.2 **Data Protection Impact Assessments (DPIA)** must be completed and approved by the Data Protection Lead(s) for any significant changes to how personal data is processed that are likely to result in a high risk to individuals and where any new technologies or systems are used. A DPIA is required, in particular, if:
installing a new CCTV system
carrying out automated decision making
carrying out a project involving large-scale processing of sensitive data

11.3 DPLs regularly spot check and review DPIAs.

12. Third party and data sharing agreements

12.1 All Oxfordshire Mind partnerships with other third-party organisations should include within the contractual agreement a clear statement as to the extent to which 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 Oxfordshire Mind and the third-party partner organisation with regard to data protection.

12.2 The signatory on the agreement, contract or statement is responsible for ensuring the following are both completed and sent to the DPL(s)
- Data Protection Impact Assessment (DPIA)
- Data sharing agreement (templates are available)

12.3 In addition, any external parties, such as contractors with access to personal data during their work, will be required to conform to Oxfordshire Mind's Confidentiality Agreement – which may be contained within another document - and must demonstrate their agreement in writing.

12.4 Oxfordshire Mind works regularly with the network of Local Minds, which are independent charities in their own right but affiliated to Mind through a membership agreement. This agreement requires all Local Minds to have their own data protection policies and procedures in place. The Agreement also requires that Local Minds evidence that they implement their data protection policy and procedures as part of the Mind Quality Mark assurance system.

13. Data Breaches

13.1 Any Oxfordshire Mind worker becoming aware of a data breaches should reported this to their manager and the Data Protection Lead(s) within 24 hours of the breach arising. Collectively they will decide how to respond to the breach and whether it needs to be notified.

13.2 The Data Breach Procedure 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 Data Protection Lead must notify the Information Commissioners Office at the soonest possible time and within 72 hours of 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.

13.3 Data breaches and remedial actions are recorded on In-Form by the DPL and updated by the line manager.

13.4 Data breaches reported to the ICO will be reported immediately to Oxfordshire Mind's CEO, Chair of Trustees and Chair of the Governance and Audit Sub-Committee.

14. Anonymisation

14.1 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.

15. Confidentiality

15.1 All confidential information pertaining to Oxfordshire Mind, its partners, and other third-party organisations, must be kept and handled confidentially, whether the information has been received formally, informally or discovered by accident (anything seen or overheard accidentally).

15.2 Examples of how to ensure confidentiality are set out below. Workers should discuss with their line manager if they have any concerns about their ability to ensure confidentiality.

Be aware of who else may be listening, particularly in areas open to the public or when home working
Clear your work area and lock your desk and /or filing cabinets at the end of each day.
Always lock your computer screen if you leave your desk unattended
If anyone comes near you while you are working with confidential information, discreetly cover the material.
If you need to take sensitive documents away from the office, seek permission from a manager first.
Do not read or process confidential documents in public places or on public transport
Only disclose and discuss information that is professionally relevant.
Double check email and postal addresses for accuracy before sending items.
Always remove printing and photocopying immediately when using a shared printer
Take care to securely destroy all unused rough work and any spare copies.
When photocopying or printing do not let anyone else read the documents, make only the required number of copies and check that nothing is left in the machine.

15.3 All workers must sign a confidentiality agreement before being given access to Oxfordshire Mind's information assets. For paid staff this agreement forms part of their contract of employment. For volunteers it is covered by Oxfordshire Mind's volunteer confidentiality pledge.