MindOut LGBTQ Mental Health Service

Data Protection Policy (Including Archiving and Retention)

1. Introduction and purpose of the policy

1.1 MindOut is required to maintain certain personal data about past and current employees, clients and service users and providers for the purposes of satisfying operational and legal obligations. We recognise that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operation.

1.2 The types of personal data that MindOut may require include information about: current, past and prospective employees; members and trustees of the Charity; clients and service users; suppliers and others with whom it communicates.

1.3 This personal data, whether it is held on paper, on computer or other media, will be subject to the appropriate legal safeguards as specified in the Data Protection Act 1998.

1.4 Data Users are obliged to comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary action.

1.5 This policy does not form part of any employee's contract of employment and may be amended at any time.

1.6 MindOut fully endorses and adheres to the eight principles of the Data Protection Act. These principles specify the legal conditions that must be satisfied in relation to obtaining, handling, processing, transportation, and storage of personal data. Employees and any others who obtain, handle, process, transport and store personal data for MindOut must adhere to these principles.

1.7 MindOut is concerned with respecting the rights of individuals when processing their personal information. This can be achieved by being open and honest with them about the use of information about them and by following good data handling procedures.

1.8 The Data Protection Compliance Manager is responsible for ensuring compliance with the Act and with this policy. [That post is held by Helen Jones, MindOut CEO. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Compliance Manager.]

2. Legal definitions used in the Data Protection Act

2.1 **Data** includes computerised and manual filing systems that are structured by reference to individuals and readily accessible, for example, card indexes, case file records.

2.2 **Data controllers** are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Act. We are the

data controller of all personal data used in our business for our own commercial purposes.

2.3 **Data users** are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

2.4 **Data subjects** for the purpose of this policy include all living individuals about whom we holds personal data save for our employees. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

Data subjects at MindOut include:

- service users
- carers of service users
- organisation contact persons
- donors (individuals or organisations)
- employees and prospective employees through recruitment
- Trustees and volunteers

2.5 **Data processors** include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on MindOut's behalf.

2.6 **Personal Data** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

2.7 **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

2.8 **Sensitive personal data** includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

3. Data Protection Principles

3.1 Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

- Processed fairly and lawfully.
- Processed for limited purposes and in an appropriate way.
- Adequate, relevant, and not excessive for the purpose
- Accurate
- Not kept longer than necessary for the purpose
- Processed in line with data subjects' rights
- Secure
- Not transferred to people or organisations situated in countries without adequate protection

4. Fair and lawful processing

4.1 The Act is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

4.2 For personal data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in the Act. These include, among other things, the data subject's consent to the processing, or that the processing is necessary for the performance of a contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, or for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, additional conditions must be met. When processing personal data as data controllers in the course of our business, we will ensure that those requirements are met.

5. Processing for limited purposes

5.1 In the course of our business, we may collect and process the personal data set out in the Schedule. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

5.2 We will only process personal data for the specific purposes set out in the Schedule or for any other purposes specifically permitted by the Act. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

6. Notifying data subjects

6.1 If we collect personal data directly from data subjects, we will inform them about:

- The purpose or purposes for which we intend to process that personal data.

- The types of third parties, if any, with which we will share or to which we will disclose that personal data.
- The means, if any, with which data subjects can limit our use and disclosure of their personal data.

6.2 If we receive personal data about a data subject from other sources, we will provide the data subject with this information as soon as possible thereafter.

6.3 We will also inform data subjects whose personal data we process that we are the data controller with regard to that data, [and who the Data Protection Compliance Manager is].

7. Adequate, relevant, and non-excessive processing

7.1 We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

8. Accurate Data

8.1 We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

9. Timely Processing

9.1 We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

10. Processing in line with data subjects' rights

10.1 We will process all personal data in line with data subjects' rights, in particular their right to:

- Request access to any data held about them by a data controller (see also Dealing with subject access requests (www.practicallaw.com/6-582-8450)).
- Prevent the processing of their data for direct-marketing purposes.
- Ask to have inaccurate data amended (see also Accurate data (www.practicallaw.com/6-582-8450)).
- Prevent processing that is likely to cause damage or distress to themselves or anyone else.

11. Data Security

11.1 We will process all personal data we hold in accordance with our Data Security Policy

11.2 We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

11.3 We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

11.4 We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

- **Confidentiality** means that only people who are authorised to use the data can access it.
- **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.
- **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on MindOut's central computer system instead of individual PCs.

11.5 Security procedures include:

- **Entry controls.** Any stranger seen in entry-controlled areas should be reported.
- **Secure lockable cabinets and cupboards.** Filing cabinets and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
- **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.
- **Equipment.** Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

12. Transferring personal data to a country outside the EEA

12.1 We may transfer any personal data we hold to a country outside the European Economic Area ("EEA"), provided that one of the following conditions applies:

- The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms.
- The data subject has given his consent.
- The transfer is necessary for one of the reasons set out in the Act, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject.
- The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.
- The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

12.2 Subject to the requirements in clause 12.1 above, personal data we hold may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. That staff maybe engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

13. Disclosure and sharing of personal information

13.1 We may share personal data we hold with any member of our group, which means subsidiaries, a holding company and its subsidiaries, as defined in section 1159 of the UK Companies Act 2006.

13.2 We may also disclose personal data we hold to third parties:

- In the event that we sell or buy any business or assets, in which case we may disclose personal data we hold to the prospective seller or buyer of such business or assets.
- If we or substantially all of our assets are acquired by a third party, in which case personal data we hold will be one of the transferred assets.
- If we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.
- We may also share personal data we hold with selected third parties for the purposes set out in the Schedule.

14. Dealing with subject access requests

14.1 Data subjects must make a formal request for information we hold about them. This must be made in writing. Employees who receive a written request should forward it to their line manager or the Data Protection Compliance Manager immediately.

14.2 When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:

- We will check the caller's identity to make sure that information is only given to a person who is entitled to it.
- We will suggest that the caller put their request in writing if we are not sure about the caller’s identity and where their identity cannot be checked.

14.3 Our employees will refer a request to their line manager [or the Data Protection Compliance Manager] for assistance in difficult situations. Employees should not be bullied into disclosing personal information.

15. Changes to this policy

15.1 We reserve the right to change this policy at any time. Where appropriate, we will notify data subjects of those changes by mail or e-mail.

Appendix 1

Archive Policy and Procedure: Introduction

Archiving Data within an organisation is an important facet to the data-protection act of 1998. In accordance to the same act and the Freedom of Information Act 2000 information needs to be held for a specific period of time.

The scope of this appendix is to give a clear guide into the length that data needs to be retained. All data retained needs to be kept in accordance with the over-arching data protection policy that this is a part of.

2. Data Schedule

Record	Statutory Retention Period	Statutory authority
Client casework records	There is no legal requirement here but MindOut's policy is 7 years	N/A
Public Liability Insurance Records	40 years	N/A
accident books, accident records/reports	3 years after the date of the last entry (see below for accidents involving chemicals or asbestos)	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR)
accounting records	3 years for private companies, 6 years for public limited companies	Section 221 of the Companies Act 1985
income tax and NI returns, income tax records and correspondence with the Inland Revenue	not less than 3 years after the end of the financial year to which they relate	The Income Tax (Employments) Regulations 1993 (SI 1993/744)
medical records and details of biological tests under the Control of Lead at Work Regulations 1998	40 years from the date of the last entry	The Control of Lead at Work Regulations 1998 (SI 1998/543)
medical records as specified by the Control of Substances Hazardous to Health	40 years from the date of the last entry	The Control of Substances Hazardous to Health Regulations 1999 (COSHH)

Regulations 1999		(SI 1999/437)
records relating to children	until the child reaches the age of 21	Limitation Act 1980
records relating to events notifiable under the Retirement Benefits Schemes (Information Powers) Regulations 1995, records concerning decisions to allow retirement due to incapacity, pension accounts and associated documents	6 years from the end of the scheme year in which the event took place, or the date upon which the accounts/reports were signed/completed.	The Retirement Benefits Schemes (Information Powers) Regulations 1995
Statutory Maternity Pay records, calculations, certificates (Mat B1s) or other medical evidence	3 years after the end of the tax year in which the maternity period ends	The Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960)
Statutory Sick Pay records, calculations, certificates, self- certificates	3 years after the end of the tax year to which they relate	The Statutory Sick Pay (General) Regulations 1982 (SI 1982/894)
wage/salary records (also overtime, bonuses, expenses)	6 years	Taxes Management Act 1970
actuarial valuation reports	Permanently	None Exist
application forms and interview notes (for unsuccessful candidates)	6 months to a year	None Exist
assessments under Health and Safety Regulations and records of consultations with safety representatives and committees	Permanently	None Exist
Inland Revenue approvals	Permanently	None Exist
money purchase details	6 years after transfer or value taken	None Exist
parental leave	5 years from birth/adoption of the child or 18 years if the	None Exist

	child receives a disability allowance	
pension scheme investment policies	12 years from the ending of any benefit payable under the policy	None Exist
pensioners' records	12 years after benefit ceases	None Exist
personnel files and training records (including disciplinary records and working time records)	6 years after employment ceases	None Exist
redundancy details, calculations of payments, refunds, notification to the Secretary of State	6 years from the date of redundancy	None Exist
senior executives' records (that is, those on a senior management team or their equivalents)	permanently for historical purposes	None Exist
time sheets	2 years after audit	None Exist
trade union agreements	10 years after ceasing to be effective	None Exist
trust deeds and rules	Permanently	None Exist
trustees' minute books	Permanently	None Exist
works council minutes	Permanently	None Exist
Records relating to persons receiving treatment for a mental disorder within the meaning of the Mental Health Act 1983	20 years after the date of last contact between the patient and any health care provider, or 8 years after the patient's death if sooner.	