# Data Protection Policy

| | |
|---|---|
| Inmind Reference: | GDPR03 |
| Category: | General Data Protection Regulation (GDPR) Policy |
| Version Number: | 1.3 |
| Reviewed on: | February 2019 |
| Next review date: | February 2020 |
| Lead Officer: | GDPR / Director of Contract Performance |
| Equality Impact Assessment completed: | Yes |

| **Applicable Legislation/Regulations:** |
|---|
| Human Rights Act 1998<br>Data Protection Act 1998<br>Common Law Duty of Confidentiality<br>Freedom of Information Act 2000<br>Access to Health Records Act 1990<br>Public Interest Disclosure Act 1998<br>Information Security Standards – ISO/IEC 17799: 2005 and IS Management NHS Code of Practice<br>General Data Protection Regulation (will apply in the UK from 25 May 2018)<br>Health and Social Care Act 2008 (Regulated Activities) Regulations 2014: Regulation 17 |
| **Codes of Practice:** |
| The Caldicott Report 1997 and '7' Guidelines<br>Records Management Code of Practice for Health and Social Care 2016 (IGA)<br>The NHS Confidentiality Code of Practice<br>Policy Statement on Information Security and Governance – CQC – July 2016 |
| **Purpose:** |
| To ensure Inmind Healthcare Group fulfils its legal duty to:<br>• Protect personal data held by the organisation, whether electronically or in paper format;<br>• Ensure personal data is processed securely and fairly in accordance with the principles of the Data Protection Act (1998). |

| **Version Control Table** | | |
|---|---|---|
| **Date Ratified** | **Version Number** | **Status** |
| February 2018 | 1.3 | Close |
| February 2019 | 1.4 | Live |

| **Date** | **Key Revision** |
|---|---|
| February 2018 | Reformatted and reviewed full policy |
| February 2018 | Addition of regulations, regulated activity and new definitions |
| February 2018 | Inserted Appendix 1 – NMC Recording Keeping |
| February 2019 | Ratified and uploaded onto new policy template. |

***Please check to ensure this is the most current electronic copy of this document as it is updated and published in electronic format only (hard copies may become out of date).***

**Equality Impact Assessment for this policy**

| Protected Characteristic (domain) | Area of conflict | Resolution |
|---|---|---|
| Age | Nil | N/A |
| Disability | Nil | N/A |
| Gender Reassignment | Nil | N/A |
| Pregnancy & Maternity | Nil | N/A |
| Race | Nil | N/A |
| Religion or Belief | Nil | N/A |
| Sex | Nil | N/A |
| Sexual Orientation | Nil | N/A |
| Marriage and Civil Partnership | Nil | N/A |

All relevant persons are required to comply with this policy and must demonstrate sensitivity and competence in relation to diversity in race, faith, age, gender, disability and sexual orientation. If you feel you are disadvantaged by this policy, please contact the Registered Manager and the service will actively respond to the enquiry.

## 1.0 The Policy

1.1 Inmind Healthcare Group holds and processes information about employees, service users, and other data subjects for administrative and commercial purposes. When handling such information, Inmind Healthcare Group, and all staff or others who process or use any personal information, must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (the Act). In summary these state that personal data shall:

- Be processed fairly and lawfully,
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with the purpose,
- Be adequate, relevant and not excessive for the purpose
- Be accurate and up-to-date
- Not be kept for longer than necessary for the purpose
- Be processed in accordance with the data subject's rights
- Be kept safe from unauthorised processing, and accidental loss, damage or destruction
- Not to be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data, except in specified circumstances.

1.2 Definitions

***"Staff", "Service Users"*** and ***"other data subjects"*** may include past, present and potential members of those groups.

***"Other data subjects"*** and ***"third parties"*** may include contractors, suppliers, contacts, referees, friends or family members.

***"Processing"*** refers to any action involving personal information, including obtaining, viewing, copying, amending, adding, deleting, extracting, storing, disclosing or destroying information.

***Personal Data*** relating to a living individual who can be identified

***Sensitive Personal Data*** consisting of information relating to;

- Racial or ethnic origin
- Political opinions
- Religious beliefs or other beliefs of a similar nature
- Information relating to physical or mental health

- Information relating to the individual's sex life
- Information relating to offences or alleged offences

***Processing (in relation to information or data)*** relates to obtaining, recording or holding the information or data, or carrying out any operation using the information or data, including;

- Organising, adapting or altering
- Retrieval, consultation or use
- Disclosure
- Aligning, combining, erasing or destroying

1.3 ***Health and Social Care Act 2008 (Regulated Activities) Regulations 2014: Regulation 17***

As in the most recent policy statement from CQC (July 2016) information security and governance – the following is the regulated activity in relation to information governance:

1. Systems or processes must be established and operated effectively to ensure compliance with the requirements in this Part.

2. Without limiting paragraph (1), such systems or processes must enable the registered person to;

   a) assess, monitor and improve the quality and safety of the services provided in the carrying on of the regulated activity (including the quality of the experience of service users in receiving those services);

   b) assess, monitor and mitigate the risks relating to the health, safety and welfare of service users and others who may be at risk which arise from the carrying on of the regulated activity;

   c) maintain securely an accurate, complete and contemporaneous record in respect of each service user, including a record of the care and treatment provided to the service user and of decisions taken in relation to the care and treatment provided;

   d) maintain securely such other records as are necessary to be kept in relation to—

      i. persons employed in the carrying on of the regulated activity, and
      ii. the management of the regulated activity;

   e) seek and act on feedback from relevant persons and other persons on the services provided in the carrying on of the regulated activity,

for the purposes of continually evaluating and improving such services;

f) evaluate and improve their practice in respect of the processing of the information referred to in sub-paragraphs (a) to (e).

3. The registered person must send to the Commission, when requested to do so and by no later than 28 days beginning on the day after receipt of the request:

a) a written report setting out how, and the extent to which, in the opinion of the registered person, the requirements of paragraph (2)(a) and (b) are being complied with, and

b) any plans that the registered person has for improving the standard of the services provided to service users with a view to ensuring their health and welfare.

## 2.0 The Procedure

### 2.1 Notification of Data Held

Inmind Healthcare Group shall notify all staff and service users and other relevant data subjects of the types of data held and processed by Inmind Healthcare Group concerning them and the reasons for which it is processed. The information which is currently held by Inmind Healthcare Group and the purposes for which it is processed when processing for a new or different purpose is introduced, the individuals affected by that change will be informed.

### 2.2 Staff Responsibilities

All staff shall:

- Ensure that all personal information which they provide to Inmind Healthcare Group in connection with their employment is accurate and up-to-date.
- Inform Inmind Healthcare Group of any changes to information, for example, changes of address.
- Check the information which Inmind Healthcare Group shall make available from time to time, in written or automated form, and inform Inmind Healthcare Group of any errors or, where appropriate, follow procedures for up-dating entries on computer forms. Inmind Healthcare Group shall not be held responsible for errors of which it has not been informed.

When staff hold or process information about service users, colleagues or other data subjects (for example, service users' course work, pastoral files, references to other

health care institutions, or details of personal circumstances), they should comply with the Data Protection Guidelines

Staff shall ensure that all personal information is kept securely and that they do not provide unnecessary access to records to others.

In practise this means:

- All files or documents of a confidential nature must be stored securely in a lockable filing cabinet and should only be accessed by employees who have a need and a right to access them.

- No files or documents of a confidential nature should be left out where they can be read by unauthorised staff or others.

- Use passwords on systems and records where appropriate and never divulge passwords to others except where this is necessary to effect formal transfer of information (e.g. in the case of a password protected document or file).

- Log off systems (or otherwise make them inaccessible to others) when leaving the computer even for a short period

- Never leave a computer with service user or other confidential information on screen and actively ensure that confidential information cannot be overseen. The use of screen savers and screen blanking should be used to facilitate this requirement.

When staff supervise service users doing work which involves the processing of personal information, they must ensure that those service users are aware of the Data Protection Principles the requirement to obtain the data subject's consent where appropriate.

2.3 **Service User Responsibilities**

All service users shall

- ensure that all personal information which they provide to Inmind Healthcare Group is accurate and up-to-date;

- inform Inmind Healthcare Group of any changes to that information, for example, changes of address;

- check the information which Inmind Healthcare Group shall make available from time to time, in written or automated form, and inform Inmind Healthcare Group of any errors or, where appropriate, follow procedures for up-dating entries on computer forms. Inmind Healthcare Group shall not be held responsible for errors of which it has not been informed.

## 2.4 Rights to Access Information

Staff, service users and other data subjects in Inmind Healthcare Group have the right to access any personal data that is being kept about them either on computer or in structured and accessible manual files.

Any person may exercise this right by submitting a request in writing to the Registered Manager, who in turn shall review the request with the Caldicott Guardian and/or Director of Governance and Compliance. No staff member should release any information in response to a Subject Access Request until they have received authorisation from the Registered Manager or Director of Governance and Compliance.

A ***subject access request (SAR)*** is simply a written request made by or on behalf of an individual for the information which he or she is entitled to ask for under section 7 of the Data Protection Act 1998 (DPA). The request does not have to be in any form. Nor does it have to include the words 'subject access' or make any reference to the DPA.

Inmind Healthcare Group will make a charge of £10 for each official Subject Access Request under the Act.

Inmind Healthcare Group aims to comply with requests for access to personal information as quickly as possible but will ensure that it is provided within 40 days unless there is good reason for delay. In such cases, the reason for the delay will be explained in writing by the Administrator to the data subject making the request.

## 2.5 Subject Consent

In some cases, such as the processing of sensitive information or the processing of research data, Inmind Healthcare Group is entitled to process personal data only with the express consent of the individual. Please also see Consent Policy.

In all cases this data must not be processed without clear permission for the person whose data it is. This applies to anyone whose data Inmind Group holds and includes but is not limited to Service Users and staff.

## 2.6 Sensitive Information

Inmind Healthcare Group may process sensitive information about a person's health, disabilities, criminal convictions, to ensure that staff are suitable for the jobs offered. Inmind Healthcare Group may also require such information for the administration of the sick pay policy, the absence policy or the equal opportunities policy.

Inmind Healthcare Group may ask for information about health needs, such as allergies to particular forms of medication, or conditions such as asthma or diabetes. Inmind Healthcare Group will only use such information to protect the health and safety of the individual, for example, in the event of a medical emergency.

2.7 **The Data Controller and the Designated Data Controllers**

Inmind Healthcare Group is the data controller under the Act, and Inmind is ultimately responsible for implementation. Responsibility for day-to-day matters will be delegated to the Managers and Administrators as designated data controllers.

Information and advice about the holding and processing of personal information is available from either the designated managers or administrators.

2.8 **Assessments**

Service Users shall be entitled to information about their assessments as soon as that information is collated and finished.

2.9 **Retention of Data**

Inmind Healthcare Group will keep different types of information for differing lengths of time, depending on legal and operational frameworks.

Below are the timescales the Inmind Group anticipate keeping such data

- Service user notes/records - 20 years from last entry
- Kitchen and Housekeeping records - 3 years
- Personnel records - 6 years
- Application forms - Duration of employment
- Payroll and tax information - 6 years
- Sickness records - 3 years
- Annual Leave records - 2 years
- Unpaid/Special Leave - 5 years
- Annual Appraisal - 5 years
- Records relating to accidents - 12 years or injuries at work

2.10 **Compliance**

Compliance with the Act is the responsibility of all service users and members of staff. Any deliberate or reckless breach of this Policy may lead to disciplinary action, and where appropriate, legal proceedings. Any questions or concerns about the interpretation or operation of this policy should be taken up with the either the designated managers or administrators.

Any individual, who considers that the policy has not been followed in respect of personal data about him- or herself, should raise the matter with the Director of Governance and Compliance initially. If the matter is not resolved it should be referred to the staff grievance or resident complaints procedure.

2.11 **Use of Electronic Records and Memory Devices**

- Registered Managers are responsible for ensuring that appropriate technical and organisational measures laid down in policies or under instruction from

the Board of Directors have been embedded to prevent unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. In practice, this means:

- Wherever possible, no data is held on the local hard drive of a computer but stored on the unit server file store.

- Incremental/full back-ups of the data held on the server file store are carried out daily/weekly.

- Data back-up discs and tapes are stored within a fireproof media safe or held off site.

- Wherever possible, no personal data should be stored on portable memory devices. If it is necessary to do so, any such data must be held on an Inmind-issued device and this data should be encrypted using the software provided.

- The Unit Registered Manager is responsible for maintaining a register of any Inmind-issued portable memory devices. Any devices taken off-site by their staff must only be done so with the agreement of the Registered Manager in consultation with the Director of Governance and Compliance.

- Any staff member/visiting professional using an Inmind-issued portable memory device must sign the register to agree that any personal data it is kept safely whilst off-site.

2.12 **Staff Data Access**

The Inmind Group reserve the right to access communications by staff using Inmind provided equipment including but not limited to mobile phone messages, emails and text messages.

This access will not be undertaken until the staff have been informed it is happening. The company will provide reasons why they are doing this, and they will undertake that such access is appropriate and proportional.

**Appendix 1**

**NMC Principles of Good Record Keeping (adapted from NMC Record Keeping: Guidance for Nurses and Midwives, 2010)**

1. Handwriting should be legible.
2. All entries to records should be signed. In the case of written records, the person's name and job title should be printed alongside the first entry.
3. You should put the date and time on all records. This should be in real time and chronological order and be as close to the actual time as possible.
4. Your records should be accurate and recorded in such a way that the meaning is clear.
5. Records should be factual and not include unnecessary abbreviations, jargon, meaningless phrases or irrelevant speculation.
6. You should use your professional judgement to decide what is relevant and what should be recorded. If necessary, seek advice from a colleague or manager.
7. You should record details of any assessments and reviews undertaken and provide clear evidence of the arrangements you have made for future and ongoing care. This should also include details of information given about care and treatment.
8. Records should identify any risks or problems that have arisen and show the action taken to deal with them.
9. You have a duty to communicate fully and effectively with your colleagues, ensuring that they have all the information they need about the people in your care.
10. You must not alter or destroy any records without being authorised to do so.
11. In the unlikely event that you need to alter your own or another healthcare professional's records, you must give your name and job title, and sign and date the original documentation. You should make sure that the alterations you make, and the original record, are clear and auditable.
12. Where appropriate, the person in your care, or their carer, should be involved in the record keeping process.
13. The language that you use should be easily understood by the people in your care.
14. Records should be readable when photocopied or scanned.
15. You should not use coded expressions of sarcasm or humorous abbreviations to describe the people in your care.
16. You should not falsify records.