DATA PROTECTION POLICY

This policy must be read in conjunction with Metanoia Institute's (the Institute) IT and Telephone Acceptable Use Policy, Bring Your Own Device Acceptable Use Policy and Disclosing Data to Third Parties guidance since all four are closely inter-linked.

1. Policy Statement and Scope

1.1. The Institute must comply with the General Data Protection Regulation (the GDPR) replacing the Data Protection Act 1998 on 25 May 2018 in relation to all personal data. The Institute has developed this policy to set out the obligations of staff and students in this regard.

1.2. The GDPR applies to processing carried out by organisations operating within the EU and organisations outside the EU that offer goods or services to individuals in the EU. The GDPR does not apply to certain activities, including:

- processing covered by the EU Law Enforcement Directive
- processing for national security purposes
- processing carried out by individuals purely for personal/household activities.

1.3. Article 5 of the GDPR - or principles relating to the processing of personal data - requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) 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 not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) 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;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is 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 subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) 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.

1.4. The policy and the GDPR apply to all personal data processed by the Institute in hard copy or electronically regardless of where the data is held and who owns the device on which it is stored so long as its processing is carried out for Institute-related purposes.

1.5. The Institute is committed to complying with the GDPR as an academic institution, an employer and a service provider. In order to do so, the Institute will:

- rely on appropriate lawful grounds for processing personal data or obtain consent when collecting it, per section 3 of this policy;
- inform staff, students and clients how their data is processed, on what grounds, for what purposes and for how long as well as who it is shared with, per section 4 of this policy;
- ensure staff are appropriately trained in managing personal data and records containing personal data is effectively managed, per section 5 of this policy.
- keep personal data safe and secure, per section 6 of this policy;
- observe the rights of individuals under the GDPR, per section 7 of this policy;

1.6. The Institute, as a body corporate, is the Data Controller under the GDPR, and the Board of Trustees, as the governing body of the Institute, is ultimately responsible for compliance with the regulation.

1.7. The Institute Data Protection Officer, who is the named contact with the Information Commissioner's Office, is Amalia Sexton based at North Common Road Campus. The Institute Data Protection Officer's responsibility is to monitor internal compliance, inform and advise on the Institute's data protection obligations and act as contact point for data subjects and the supervisory authority.

1.8. The Information Commissioner's Office website contains a wide range of policy and guidance around Data Protection.

2. Definitions

2.1. **Personal data** is any information relating to an individual who can be directly or indirectly identified by reference to its name, identification number, location of data or online identifier. The GDPR applies to both automated personal data and to manual filing systems where personal data is accessible according to specific criteria; for example, chronologically ordered sets of manual records containing personal data.

2.2. **Special category personal data** are sets of sensitive personal data relating to the race or ethnic origin, political opinion, religious belief, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life or sexual orientation of an individual. The GDPR rules for sensitive data do not apply to information about criminal

allegations, proceedings or convictions but separate safeguards for this type of personal data is required.

2.3. **Confidential data** is information given in confidence or agreed to be kept confidential and therefore not in the public domain. Some confidential data may also be personal data and/or special category personal data and therefore fall within the scope of this policy. The Institute also handles research data which comprises materials collected or created for the purposes of analysis to generate original research results, some of which may contain personal data and/or special category personal data; the scope of this policy applies in all such cases.

2.4. **Data subject** is the individual whose personal data is being processed.

2.5. **Data processing** is widely defined and includes every possible form of action that may be undertaken in relation to data, including:

- obtaining information
- recording information
- keeping information
- using information in any way
- sharing or disclosing information
- erasing and/or destroying information.

2.6. A **controller** is any individual or organisation who determines the purposes and means of processing personal data. Controllers are not relieved of their obligations where a processor is involved as the regulation places further obligations on them to ensure their contract with processors complies with the GDPR.

2.7. A **processor** is any individual or organisation who processes personal data on behalf of the controller. If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of the personal data you hold and your processing activities. You will have a legal liability if you are responsible for a breach.

3. Legal Framework

3.1. The Institute processes personal data about its staff, students and clients for a variety of reasons, such as to recruit and pay its staff; to enrol and record the academic progress of its students; to provide clinical services; for direct marketing purposes; and to comply with statutory obligations such as the Health & Safety at Work etc. Act 1974, the Rehabilitation of Offenders Act 1974 or the Equality Act 2010.

3.2. In order for the Institute to process data 'fairly', we will:

- ensure that we have a legitimate reason to obtain and process the data

- make the data subject aware that their data is being used and their consent obtained; they must have a clear understanding of the reasons for which the Institute processes their data and must never be deceived or misled
- obtain express consent from data subjects to process special category data
- ensure that personal data is only obtained from a data subject who is legally authorised to provide it

3.3. The following activities are strictly prohibited:

- using data obtained for one purpose for a supplemental purpose e.g. using contact details provided for HR-related purposes for marketing purposes
- disclosing personal data to a third person outside of the Institute without the consent of the data subject

3.4. Personal data will be shared only within the EU (currently 28-member states), plus three EEA countries which have agreed to be bound by the EU Data Protection Directive (Norway, Liechtenstein, and Iceland); and also the following countries which have been judged by the EU to afford 'an adequate level of protection' of personal data (currently, Switzerland, Canada, Argentina, Guernsey, Jersey, Andorra, Faroe Islands, Israel and the Isle of Man).

4. Data Protection Notification

4.1. The Institute takes its obligations under the GDPR very seriously and will always ensure personal data is collected, handled, stored and shared in a secure manner.

4.2. The Institute's Recruitment Data Privacy Statement and Privacy Notice outline what personal data we collect, the lawful bases for collecting it, how we use it, how long we keep it and with whom we share it. It also provides guidance on individual subject rights and how to make a complaint to the Information Commissioner's Office, the regulator for data protection in the UK.

5. Managing Data in Compliance with the GDPR

5.1. Whenever data is gathered or collected under GDPR for Institute-related purposes, including data obtained for academic research, we must comply with the GDPR.

5.1.1. Gathering data

- only collect the personal data you need – ask yourself if you can achieve the same purpose with less information
- tell your data subjects in clear terms and preferably in writing what information is being collected, on what bases, for what purposes and with whom it may be shared
- keep a record of your data subjects' consent to their data being processed
- keep the data you have collected secure in accordance with the guidelines found within section 6 of this policy

5.1.2. Keeping and maintaining data

- **Accuracy.** Records must be kept up-to-date and regularly checked for accuracy; you must record any changes and delete any obsolete information
- **Relevance.** Only keep relevant and necessary records; carry out regular administration of files and records to remove duplicates and irrelevant information
- **Fairness and access rights.** Individuals have the right to see their personal data, including any comments about them. Therefore, opinions about individuals should be justifiable and based on fact; you must not record any comments you would not be happy for the data subject to view
- **Limit access to data.** Restrict access to those staff or individuals who require access for legitimate business or operational reasons
- **Only use data for the original purpose.** Data collected for one purpose cannot be used for another without the individual's knowledge and consent
- **Keep files in a single location.** Information and documents containing personal data to be referred to or used for Institute-related purposes should be kept centralised in a single location e.g. CRM or appropriate network drive. In order to avoid duplication or fragmentation of information, no private files should be held and where necessary, they should be deleted or disposed of securely after the employment/training/service ceases e.g. a tutor holds a 'private' file to record student progression for the duration of the training
- **Only retain data for as long as necessary.** When employment/training/service ceases, the relevant file is closed. Files must be weeded and records with no further use disposed of in accordance with the specified Record Retention Schedule. Confidentiality must be maintained at all times when personal data is disposed of and in accordance with the guidelines found within section 6 of this policy

5.1.3. Disclosing data

- Individuals have the right to see all information held about them
- Personal data should only be disclosed to third parties within or outside the Institute, including members of staff, partners or sponsors; if they have a legitimate reason to access the information and only with consent from the data subject
- You should take steps to ensure that requests from officials such as the police or the Inland revenue are genuine and legitimate e.g. the police use a standard form to request personal information
- Any non-routine request(s) should be referred to the Data Protection Officer
- Personal information can be disclosed to medical staff without consent only in an emergency e.g. the data subject collapses or is unconscious
- See Disclosing Data to Third Parties for further guidance

6. Data Security

6.1. Any information staff and students access when conducting Institute business that pertains to individuals is covered by the GDPR. The regulation applies to personal data processed on site and remotely or on mobile devices, irrespective of who the device belongs to as long as

the personal data is accessed for Institute business. If mobile devices and home computers are used to access Institute emails, there is likely to be personal data within the emails that falls under the GDPR.

6.2. Staff and students can avoid the most common causes of data loss and breaches by adhering to the following:

6.2.1. **Always keep personal data secure**

- keep paper files in locked cabinets/drawers or locked offices when not in use and stored securely at the end of business – never leave paper files on desks
- lock your office when left unattended during meetings or breaks
- log off or lock your computer screen when away from it
- use password protection or encryption for electronic files/documents containing special category data
- take special care when transferring personal data onto a memory stick, laptop or any other mobile device – use password protection and encryption where appropriate
- when including personal data in an email, use password protection or encryption where appropriate
- change your password frequently and adhere to the Institute's IT and Telephone Acceptable Use and Bring Your Own Device Acceptable Use policies
- don't copy personal data unless absolutely necessary
- deal with any payment information in a timely manner and dispose of the information securely once work is completed
- when taking payment information over the telephone, ask the caller to repeat the information if something is unclear – do not repeat any of the information in front of others with no legitimate right to access it
- never discuss personal information about individual(s) who are members of staff / students / clients of the Institute in front of others with no legitimate right to access such information

6.2.2. **Restrict access to personal data**

- access to personal data should only be granted to Institute staff who have legitimate reasons to access it
- personal data must not be disclosed to third parties without express consent from the data subject
- unauthorised third parties must not be able to view digital screens displaying personal data
- if you need to share personal data with a third party for business purposes, please contact the Data Protection Officer to ensure a data sharing agreement is in place

6.2.3. **Store personal data securely**

- whenever possible, store personal data on a computer server
- never store personal data on a mobile device or home computer unless necessary and the device has been encrypted where appropriate

- don't store or transfer personal data where there is a risk that it will be lost or exposed e.g. on unencrypted USB drives, mobile devices or laptops

6.2.4. **Dispose of personal data carefully**

- shred paper files or dispose of them securely using the Institute's confidential waste bins
- if you store personal data on your own device, you must securely erase it before disposing of it

6.2.5. **Report data breaches**

- the Institute has an obligation under GDPR to maintain a record of all data breaches and to report certain breaches to the Information Commissioner's Office within 72 hours of their occurrence
- all data breaches must be reported immediately to the Data Protection Officer as soon as you become aware of them, including lost or stolen laptops, memory sticks or other mobile devices as well as accidental disclosures of information e.g. sending an email containing personal data to the wrong recipient
- consult the guidance on Reporting a Data Breach for additional information

6.3. Taking personal data off-site should be considered a short-term measure. No personal data should be taken off-site without authority and having first considered its security as follows:

- use the Institute's email account for all Institute business
- reduce risks of a breach by limiting the amount of personal data taken off-site, making a copy of the data rather than using the original and wherever possible anonymising it and removing special category data or other sensitive information
- personal data stored or transferred onto a mobile device, PC or laptop outside of the Institute's IT systems must be password protected and encrypted where appropriate; and the devices or PC must be adequately protected against viruses
- special care must be taken when transporting personal data to and from home and when using public transport

7. Rights of Individuals

7.1. The Institute must comply with the GDPR in providing the following rights for data subjects:

7.1.1. Right to be informed

- Individuals must be provided clear information about the purpose(s) of processing their personal data, their retention periods, with whom the data will be shared and their rights
- This information must be provided at the point of data collection
- Privacy notices must be reviewed regularly, and any new uses brought to the attention of the Data Protection Officer and the data subjects before the processing starts

7.1.2. Right of access

- Data subjects have the right to access their personal data and supplementary information to be aware and verify the lawfulness of the processing

- All Subject Access Requests must be forwarded to the Data Protection Officer to coordinate the gathering of information
- Upon receipt of a Subject Access Request, the Institute will provide one copy of the specified information free of charge within one month of receipt of the request; additional copies may be provided at an additional cost
- Information will only be provided using reasonable (and secure) means after verifying the identity of the person making the request

7.1.3. Right to rectification

- Data subjects have the right to have personal data rectified if it is inaccurate or incomplete
- All requests for rectification must be actioned within one month of receipt of the request
- Where personal data has been shared with others, you must contact each recipient to inform them of the rectification e.g. Middlesex University; unless this proves impossible or involves disproportionate effort

7.1.4. Right to erasure, also known as 'right to be forgotten'

- Requests to be forgotten must be actioned where:
  - the personal data is no longer necessary for the purpose for which it was originally collected
  - the individual withdraws consent
  - the individual objects to the processing and the Institute has no overriding legitimate interest to continue the processing
  - the personal data was unlawfully processed
- All requests to be forgotten must be forwarded to the Data Protection Officer
- The Institute can refuse to comply with a request for erasure if the personal data is processed to exercise the right of freedom of expression and information; to comply with a legal obligation in the public interest; or to exercise or defend legal claims
- Where personal data has been shared with others, you must contact each recipient to inform them of the erasure e.g. Middlesex University; unless this proves impossible or involves disproportionate effort

7.1.5. Right to restrict processing

- Data subjects have the right to block or suppress processing of personal data
- All requests to restrict processing must be forwarded to the Data Protection Officer
- Staff and students must restrict processing where:
  - a data subject contests the accuracy of personal data until its accuracy has been verified
  - a data subject has objected to the processing whilst the Institute considers whether its legitimate grounds override those of the individual
  - processing is unlawful, but the data subject opposes erasure
  - the Institute no longer needs the personal data, but the individual requires it to establish, exercise or defend a legal claim

7.1.6. Right to data portability

- This right only applies to personal data provided to the Institute based on the individual's consent or for the performance of a contract, when processing is carried out by automated means
- Personal data must be transferred free of charge in a commonly used machine-readable form e.g. CSV files
- Requests for data portability must be actioned within one month

7.1.7. Right to object

- Individuals have the right to object to processing based on legitimate interests or the performance of a task in the public interest; direct marketing; and processing for purposes of scientific/historical research and statistics
- All objection to processing requests must be forwarded to the Data Protection Officer
- Staff and students must stop processing personal data as soon as they receive an objection

8. Responsibilities of Staff, Students and Clients

8.1. The Executive Officer is the nominated processor for all post, both internal and external, sent to or within Metanoia Institute; which is not addressed directly to members of staff. The Executive Officer opens unaddressed external post and sends it to its intended recipient, where it is treated in accordance with the principles set out in this policy document.

8.2. Compliance with the GDPR is the responsibility of all members of the Institute. Staff and students must ensure that they are familiar with the GDPR and the Institute's Data Protection Policy and related documents, which they are expected to abide by.

8.3. Any breach of the GDPR and the Institute's Data Protection Policy, whether deliberate or through negligence, may lead to disciplinary action being taken, or access to the Institute facilities being withdrawn, or even a criminal prosecution.

8.4. All staff are responsible for:

- checking that any information they provide in connection with their employment is accurate and up-to-date
- informing HR of any errors or changes

8.4.1. Staff whose work involves the management of student personal data must ensure they observe the six data protection principles of the GDPR and comply with the Institute's Data Protection Policy and any amendments or supplementary guidance issued from time to time.

8.4.2. Staff whose work includes responsibility for supervision of students' academic work and/or placements have a duty to ensure that students observe the six principles of the GDPR and comply with the Institute's Data Protection Policy and any amendments or supplementary guidance issued from time to time.

8.4.3. All staff must ensure that any holding or processing of personal data is included in the Institute's privacy notices. All new personal data being collected or new purpose(s) for processing personal data must be reported to the Data Protection Officer prior to its collection and/or processing.

8.5. Students are responsible for:

- ensuring that all personal data provided to the Institute is accurate and up to date
- informing the relevant Academic Coordinator of any errors or changes
- students who, in the course of their programme of study, process personal data must do so in accordance with the provisions of the GDPR, the Institute's Data Protection Policy and any amendments or supplementary guidance issued from time to time

8.5.1. Students who are undertaking placements and/or research projects using personal data must ensure that:

- the client/research subject is informed of the nature of the research and consents to their personal information being used
- their Supervisor is informed of the proposed research before it begins, and ensures that the Institute is licensed to undertake this kind of research
- all personal data is kept securely

8.6. All clients are responsible for:

- checking that any information they provide in connection with their access to MCPS is accurate and up-to-date
- informing the Clinical Office of any errors or changes

8.7. Personal names, the Institute telephone numbers, and email addresses may be published on the Institute's external website, unless the individual concerned informs the Data Protection Officer, in writing, that they do not wish this information to be disseminated in this way.

8.8. Staff responsible for producing pages for the external website must ensure that any individual named on those pages has not refused permission to publish their details, by checking either with the individual or with the Data Protection Officer.

Date of Revision	June 2019
Author(s)	Amalia Sexton on behalf of GDPR Task Group
Date of publication	23 May 2018
Senior Management sponsor	Chief Executive Officer