DISCLOSING DATA TO THIRD PARTIES

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

1. Important considerations

1.1. Staff and students must carry their Institute I.D. card at all times while on Institute premises and produce it on request by any staff member.

1.2. Visitors to the Institute are not allowed to roam around the building unescorted. When staff / students are ready to receive them, visitors should be escorted to a private room for further discussion so as to preserve the right to the confidentiality of their information.

1.3. 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; and must be adequate, relevant and limited to what is necessary in relation to the purpose for which it was requested.

1.4. Always exercise caution when dealing with requests from outside of the Institute for disclosing personal data and/or while discussing matters related to individual(s) who are member(s) of staff, students or clients of Metanoia Institute (the Institute) in open or public spaces.

1.5. When responding to written requests via email, ensure that the email is password protected and where appropriate encrypted.

1.6. The Institute's reserves the right to disclose information to public and official bodies without the express consent of data subjects where it has concerns about the safeguarding of those individuals.

2. Requests by telephone

2.1. Personal data should only be disclosed over the telephone in emergencies and other legally permitted circumstances.

2.2. You should neither confirm nor deny that an individual is a member of staff / student / client of the Institute. You should never feel pressured into disclosing personal data over the telephone; instead, ask the caller to put their request in writing and adhere to the guidance provided in sections 3-5 below when you have received the written request.

3. Requests from public and official bodies

3.1. Staff and students who deal with routine requests from public and official bodies must ensure that:

- the person is who they say; if you doubt the authenticity of the enquiry, please contact the Data Protection Officer to seek advice

- the enquiry is genuine; unless familiar with names, you must call back a main switchboard number to verify the legitimacy of a query

- the person whom the enquiry is about is clearly identified

3.2. All requests in writing must be on official headed paper.

3.3. Keep a record of telephone calls with any available correspondence and a copy of your response. Do not release the information until you have been able to verify the legitimacy of the request.

4. Requests from the police

4.1. The police do not have an automatic right to receive information about staff, students or clients. You should not feel pressured into disclosing personal data to the police.

4.2. Police requests to access personal data for crime-related purposes must be forwarded to dataprotection@metanoia.ac.uk.

5. Requests from other third parties

5.1. If you need to share personal data with a third party for business purposes, please contact dataprotection@metanoia.ac.uk to ensure a written data sharing agreement is in place.

5.2. The data sharing agreement ensures that the third-party processor only processes the personal data in accordance with our instructions and in compliance with GDPR. No personal data can be shared with a third-party processor until an agreement is signed by all relevant parties; and all agreements must be drafted by the Institute under appropriate legal consultation.

5.3. Former students / staff

- Requests for letters confirming enrolment /employment status or details of an award must be in writing and cannot be actioned until the identity of the individual has been verified

- It is strictly prohibited to share contact details of current and/or former students / staff with former students / staff (or anyone claiming to be one); you may however offer to forward the message to anyone matching the details provided

5.4. Other institutions / employers

- Staff may confirm the details of an award (degree type, subject, classification and date) or employment details (dates, mode and position held) on receipt of a written request by another university/training institution or employer without the data subject's signed authorisation but nothing else without their written permission

5.5. Relatives

- When someone claiming to be the spouse/partner/parent or relative of a member of staff / student / client calls asking for information, write their details and advise them that you are unable to assist them due to data protection legislation

- Contact the relevant member of staff/student/client with this information, noting that the Institute will not disclose any information to third-parties without written consent; and encourage them to contact them directly