

Recruitment Data Privacy Statement



The UK General Data Protection Regulation (UK GDPR) protects the rights of individuals by setting out certain rules as to what organisations can and cannot do with information about people. A key element to this is the principle to process individuals' data lawfully and fairly. In order to meet the fairness part of this we need to provide information on how we process personal data.

Metanoia Institute takes its obligations under the UK General Data Protection Regulation very seriously and will always ensure personal data is collected, handled, stored and shared in a secure manner. The Institute is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

The following statement outlines the different personal data we collect about you for recruitment purposes and why, how it is used and with whom we share it. The statement also provides guidance on your individual rights and how to make a complaint to the [Information Commissioner's Office](#), the regulator for data protection in the UK. As such, the statement is divided into the following sections:

1. What personal data does the Institute process for recruitment purposes and why?
 - 1.1. Prospective Employees
 - 1.2. Prospective Students
2. How does the Institute safeguard personal data?
3. Special Categories of Data
4. With whom does the Institute share personal data?
5. How long does the Institute keep personal data?
6. Your rights
7. How to Complain

The Institute's official contact details are:

Data Protection Officer
Metanoia Institute
13 North Common Road
Ealing
London
W5 2QB
Tel: +44 (0)20 8579 2505
Email: dataprotection@metanoia.ac.uk

1. What personal data does the Institute process and why?

1.1. Prospective Employees

1.1.1. The Institute collects and processes a range of information about you in order to manage the recruitment process, namely:

- your name, address and contact details, including email address and telephone number, date of birth and gender;
- details of your qualifications, skills, experience and employment history;
- information about your current level of remuneration, including entitlement to benefits such as pensions or insurance cover;
- information about your entitlement to work in the UK;
- information about medical or health conditions, including whether or not you have a disability for which the organisation needs to make reasonable adjustments;
- equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief.

1.1.2. The Institute collects this information in a variety of ways. For example, data is collected via the application form or CV; obtained from your passport or other identity documents; or through interviews, interview meetings or other forms of assessment.

1.1.3. In some cases, the Institute collects personal data about you from third parties, such as references supplied by former employers, information from employment background check providers and information from criminal records checks permitted by law and with your consent; and only when a job offer has been made.

1.1.4. The Institute needs to process data to take steps at your request prior to entering into a contract with you. It also needs to process your data to enter into a contract with you.

1.1.5. In some cases, the Institute needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check a successful applicant's eligibility to work in the UK before employment starts.

1.1.6. In other cases, the Institute has a legitimate interest in processing personal data during the recruitment process and for keeping records of the process. Processing data from job applicants allows the Institute to:

- manage the recruitment process;
- assess and confirm a candidate's suitability for employment and decide to whom to offer a job;
- respond to and defend against legal claims.

1.1.7. Where the Institute relies on legitimate interests as a reason for processing data, it has considered whether or not those interests are overridden by the rights and freedoms of employees or workers and has concluded that they are not.

- 1.1.8. The Institute processes health information if it needs to make reasonable adjustments to the recruitment process for candidates who have a disability. This is to carry out its obligations and exercise specific rights in relation to employment.
- 1.1.9. Where the Institute processes other special categories of data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is for equal opportunities monitoring purposes.
- 1.1.10. For some roles, the Institute is obliged to seek information about criminal convictions and offences. Where the institute seeks this information, it does so because it is necessary for it to carry out its obligations and exercise specific rights in relation to employment.
- 1.1.11. Metanoia Institute will not use your data for any purpose other than the recruitment exercise for which you have applied.

1.2. **Prospective Students**

- 1.2.1. The Institute collects and processes a range of information about you in order to manage the recruitment process, namely:
 - your name, address and contact details, including email address and telephone number, date of birth and gender;
 - details of your qualifications, skills, experience, employment history and professional membership information;
 - information about your entitlement to study in the UK, including nationality and passport or other identification document as well as visa information where applicable;
 - information about medical or health conditions, including whether or not you have a disability for which the organisation needs to make reasonable adjustments;
 - equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief;
 - criminal convictions information;
 - references.
- 1.2.2. The Institute also collects personal data about you from third parties, such as references supplied by former employers and/or training institutions and information from criminal records checks permitted by law and with your consent.
- 1.2.3. Data is collected during the enquiry and the recruitment processes through application forms or CVs; obtained from your passport or other identity documents; or through interviews, meetings or other forms of assessment; in order to communicate with prospective students and to make appropriate admission offers; as well as to monitor equality and diversity objectives within the Institute as indicated in its [Access and Participation Statement](#). It also needs to process your data to enter into a contract with you.

- 1.2.4. In some cases, the Institute needs to process data to ensure that it is complying with its legal obligations. For example, the Institute is required to check a prospective student's eligibility to study in the UK before the course starts; information is also required to monitor equality and diversity objectives within the Institute as well as to safeguard vulnerable adults.
- 1.2.5. In other cases, the Institute has a legitimate interest in processing personal data during the recruitment process and for keeping records of the process. Processing data from prospective student applicants allows the Institute to:
- plan and account for the use of the services provided;
 - manage the recruitment process;
 - monitor, develop and update the Institute admissions policy to ensure it continues to operate effectively;
 - assess and confirm a candidate's suitability for study and decide to whom it should make an admission offer;
 - respond to and defend against legal claims.
- 1.3. Recruitment processes are not based solely on automated decision-making.

2. How does the Institute safeguard personal data?

- 2.1. The Institute takes the security of your data seriously. The organisation has internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed or damaged, misused or disclosed, and is not accessed except by its employees in the performance of their duties. More details can be found in the Institute's [Data Protection](#), [IT and Telephone Acceptable Use](#) and [Bring Your Own Device Acceptable Use](#) policies and related guidance.
- 2.2. Prospective Employees
- 2.3. Your data is locked away in cabinets within an office with restricted and supervised access during office hours and locked after business hours; and on the HR Management systems restricted to HR access e.g. file and IT systems.
- 2.4. Where the Institute engages third parties to process personal data on its behalf e.g. payroll, they do so on the basis of written instructions, are under a duty of confidentiality and obliged to implement appropriate technical and institutional measures to ensure the security of data.
- 2.5. Prospective Students
- 2.5.1. Your information is locked away within an office with restricted access during office hours and locked when not in use; on the Registry systems, accessed by the relevant administrative and support services staff under strict control by the Institute's Registrar and the Data Protection Officer.
- 2.5.2. Where the Institute shares information with third-party service providers (please email dataprotection@metanoia.ac.uk to obtain a copy of the terms and conditions of use), they do so on the basis of a service agreement, are under a duty of

confidentiality and obliged to implement appropriate technical and institutional measures to ensure the security of data.

3. Processing 'Special Categories' of Data

- 3.1. Your personal data may include 'special categories of data' as described under the UK GDPR. Such special categories include racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
- 3.2. Metanoia Institute may process data relating to criminal convictions (e.g. if a course requires a Disclosure and Barring Service check or a student or staff member has an unspent conviction).
- 3.3. The special category data, such as ethnicity, religion or belief, are used for monitoring, statistical and research purposes in order to improve student satisfaction and attainment and ensure equality of opportunity and inclusion.
- 3.4. **HESA returns:** If you accept your offer of study with us, we are required to return important information (that will include your personal data) to HESA. Please see [HESA's collection notices](#) together with other supporting information.
- 3.5. The Institute will put particular safeguards in place for the processing of special categories" of data (see detailed information on data which falls under this definition on the [ICO website](#)).
- 3.6. The lawful basis for processing special categories of data include:
 - Consent:** The Institute will process certain sensitive information about you with your consent for example the use of ethnicity to ensure that you are not disadvantaged
 - Necessary for reasons of substantial public interest:** This includes monitoring according to characteristics such as ethnicity or disability to ensure equality of opportunity. This is also the basis for processing data in relation to counselling.
 - Necessary for the purposes of preventive or occupational medicine, medical diagnosis, the provision of health or social care or treatment:** This would relate to the provision of support plans and services through Student Services (or HR for staff).

4. With whom does the Institute share personal data?

- 4.1. Prospective Employees
 - 4.1.1. Your information will be shared internally on a 'need-to-know' basis with members of the HR and recruitment team, interviewers involved in the recruitment process, managers in the business area relating to the advertised vacancy you are applying for, and IT staff if access to the data is necessary for the performance of their roles.
- 4.2. The Institute will not share prospective employee's data with third parties, unless your application for employment is successful and it makes you an offer of employment. The Institute will then share your data with former employers to obtain references for you, employment background check providers to obtain necessary background checks and the Disclosure and Barring Service to obtain necessary criminal records checks.

4.3. Prospective Students

- 4.3.1. Your information will be shared internally on a 'need-to-know' basis with members of the student records administration and recruitment teams, including the relevant Head of Programme or relevant members of the academic Senior Management Team, if access to the data is necessary for the performance of their roles. The personal data that is shared will always be limited to what the staff member needs for the performance of their role.
- 4.3.2. The Institute is required to share your data with certain organisations in order to meet statutory requirements. Sharing will always be undertaken in line with the requirements of data protection law and with your consent. The personal data that is shared will always be limited to what the other organisation needs to meet its requirements or deliver its services.
- 4.3.3. The information below outlines the key partners with whom the Institute would share personal data of prospective students with their consent:
 - the [Office of the Independent Adjudicator](#) (OIA) to review complaints that have progressed to external scrutiny;
 - the [Information Commissioner's Office](#) (ICO) for the purpose of providing necessary information in the event of a cause for concern raised by you.
- 4.3.4. Where we share information outside of the European Economic Area, we ensure that appropriate safeguards are in place to protect your personal data. See our Privacy and Cookies Policy and our Data Protection Policy for more information.

5. How long does the Institute keep personal data?

- 5.1. The Institute takes its obligations under the UK GDPR very seriously in terms of not holding onto personal data for any longer than is necessary.

5.2. Prospective Employees

- 5.3. If your application for employment is unsuccessful, the Institute will hold your data for 6 months after the end of the appropriate recruitment cycle. The Institute has a [Record Retention Schedule](#) in place for the different categories of data it holds.

5.3.1.

- 5.3.2. If your application for employment is successful, personal data gathered during the recruitment process will be transferred to your personnel file and retained during your employment. The periods for which your data will be held will be provided to you in a new privacy notice.

5.4. Prospective Students

- 5.4.1. If your application for study is unsuccessful, information held in the Institute's registry systems will be held in line with its [Record Retention Schedule](#).

- 5.4.2. If your application for study is successful, personal data gathered during the recruitment process will be transferred to your student file and retained in accordance with the Institute's [Privacy Notice](#) and [Record Retention Schedule](#).
- 5.4.3. Where the Institute relies on legitimate reasons to process anonymised statistical information related to recruitment, selection and admission; for example, in order to monitor the fairness and effectiveness of its admissions policy; it seeks to retain the anonymised statistical data indefinitely.

6. Your Rights

- 6.1. You are under no statutory or contractual obligation to provide data to the Institute during the recruitment process. However, if you do not provide the information, the organisation may not be able to process your application properly or at all.
- 6.2. The lawful basis that the Institute uses for the processing of your personal data can affect which rights are available to you.

Lawful basis	Right of Access	Right to Rectification	Right to Restrict	Right to Erasure	Data Portability	Right to Object
Consent	✓	✓	✓	✓	✓	✗ ¹
Legal Obligation	✓	✓	✓	✗	✗	✗
Legitimate Interest	✓	✓	✓	✓	✗	✓

- 6.3. As the Data Subject (whose personal information we process) you have the right to withdraw consent from the processing of your personal data by the Institute at any time, if your consent was sought to use your personal data.

6.4. Right of Access

- 6.4.1. You have the right to ask the Institute what personal data we hold about you, and to ask for a copy of that data. This is called making a Subject Access Request.
- 6.4.2. A [Subject Access Request](#) should be submitted in writing to the Data Protection Officer (dataprotection@metanoia.ac.uk) or in hard copy to the postal address provided earlier.
- 6.4.3. The Institute reserves the right to ask you to provide proof of identification and for you to clarify your request if it is unclear in the first instance. You will receive a reply no longer than 30 calendar days from the date you make the request in writing.

¹Rather than a right to object, the individual has a right to withdraw consent

6.4.4. If you are unhappy with the initial response you can ask the Institute to undertake a further search if there is specific information you have good reason to believe exists but that hasn't been provided.

6.5. **Right to rectification**

6.5.1. If you believe the Institute holds information about you that is factually incorrect, please contact:

- The Registrar (registrar@metanoia.ac.uk) if you are a prospective student, or
- Human Resources (hr@metanoia.ac.uk) if you are a prospective employee

6.5.2. The Institute should update your record within one calendar month.

6.5.3. You must submit your request in writing as indicated above or in hard copy to the postal address provided above.

6.5.4. The Institute reserves the right to ask you to provide proof of identification and for you to clarify your request if it is unclear in the first instance. You will receive a reply no longer than 30 calendar days from the date you make the request in writing.

6.6. **Right to erasure**

6.6.1. You have a right to have personal data erased and to prevent processing in specific circumstances:

- where you believe that the personal data is no longer necessary in relation to the purpose for which it was originally collected and processed;
- when you withdraw consent;
- when you object to the processing and the Institute has no overriding legitimate interest for continuing the processing;
- when your personal data was unlawfully processed, or the Institute is found to be in breach of UK GDPR in relation to your personal data.

6.7. **Right to restrict processing**

6.7.1. The Institute will block the processing of your personal data in the following circumstances:

- when you contest the accuracy of the personal data we hold about you;
- when you object to the processing of any personal data that we hold about you for the legitimate reasons in the public interest unless the Institute has legitimate grounds to override your request;
- when processing is unlawful, but you do not wish to exercise the right to erasure;
- when you require the data to defend a legal claim despite the Institute no longer needing the data.

6.8. **Right to data portability**

6.8.1. You have the right to obtain and reuse the personal data that you have provided to the Institute based on consent, or for the performance of a contract if the processing is carried out by automated means.

6.9. **Right to object**

- 6.9.1. You have the right to object to the Institute's processing of the following:
- 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.
- 6.9.2. The Institute reserves the right to refuse your request(s) if it can demonstrate legitimate grounds for the processing which override your rights or if the processing is for the defence of legal claims.

7. **How to Complain**

- 7.1. If you believe your request has not been dealt with properly or you have a complaint to raise against the Institute for any other data protection related issue, you can contact the [Information Commissioner's Office](#) (ICO). A complaint can be raised via their [website](#) or in writing to the following address:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
SK9 5AF