Job Applicants Privacy Notice

1. Data Controller

University of Northumbria at Newcastle ("we", "our", "us") is a registered Data Controller (**Registration Number:** Z7674926) with the Information Commissioner's Office ('ICO').

2. Overview

This privacy notice describes how and why we process personal data in accordance with our obligations under the UK General Data Protection Regulation ('UK GDPR') in relation to any individual ("you", "your") as a prospective applicant or job applicant in relation to employment at Northumbria University, including Governors, self-employed and contracted personnel, temporary staff, or voluntary workers.

3. What categories of personal data are processed by us?

For purposes of this Privacy Notice, personal data means any information about an identifiable individual. Personal data excludes anonymous or de-identified data that is not associated with a particular individual. The categories of personal information we may collect, store, and use about you, include (but are not limited to):

Potential Applicants

If you join our 'Talent Community' online portal to set up filtered job alerts, you will be prompted to supply details of the jobs you are interested in hearing about and your contact information:

Data Category	Example
Contact	Name, title, addresses, telephone numbers, and personal email addresses.

You may also choose to upload a CV (resume) or covering letter containing biographical information such as your *education, training and employment history and any other data you choose to include*.

Job Applicants

If you submit a job application the following categories of data may be processed to carry out our recruitment activities:

Data Category	Example
Contact	Name, title, addresses, telephone numbers, and personal email addresses.
Biographical	Date of birth, gender, nationality, country of domicile. Current salary and notice period.
Administrative	Enquiry and correspondence records, application records (references, assessments, interview notes, offer letters), contracts and terms and conditions of employment.

Compliance and Verification	References and qualifications. Copies of driving licences, passports, visas, residence permits, or any other documents required for Home Office compliance.
Equality and Diversity Data	Special Category data, including – racial or ethnic origin, age, disability, gender reassignment, marriage and civil partnership, religion or belief, sex, and sexual orientation.
Criminal Offence Data	Relevant data relating to criminal convictions and offences
Security Data	Building entry, CCTV images.
Website Visits	Your Internet Protocol (IP) address, location data, login information, time-zone setting, weblogs, cookies and other communication data, and the resources that you access. For more information, please see our Cookies Notice

4. Where do we get your personal data from?

You may provide information to us as part of an enquiry, at a recruitment fair, by registering with the 'Talent community' or as part of the application process. Such data may be collected through the online portal, via telephone or other conversations and in the exchange of correspondence with our staff.

We may collect information from third parties acting on your behalf, such as (but not limited to):

- Nominated referees.
- Recruitment agencies (including those engaged by us)
- Former employers or educational establishments
- Social media (e.g., LinkedIn)
- Relevant online resources (e.g., ResearchGate or profile on current employer's website etc.)
- Professional Bodies
- Disclosure and Baring Services (where relevant to the position applied for)
- Credit and background checking agencies

We may also create new personal data about you as part of the assessment process.

5. Activities we process your personal data for and the lawful basis.

Your personal data will only be processed for activities relevant to the enquiry or application process as required to complete the task and only where it has been identified as 'lawful' for us to do so. Broadly speaking, the lawfulness of processing will be under one of the following lawful basis:

- Where necessary to potentially enter into a contract that we have entered into with you (e.g., Processing your application to enter into an employment contract)
- Where we need to comply with a legal obligation (e,g., right to work and immigration checks etc.)
- Where it is necessary for our legitimate interests or your interests, and where your fundamental rights do not override those interests (e.g., processing unsolicited applications, shortlisting candidates etc.)
- Where required to carry out a task in the public interest (e.g., equal opportunities monitoring and reporting)

Consent or 'Explicit Consent'

We will only rely on consent as a legal basis for processing your personal data for limited purposes for example, where we are collecting special category data for internal monitoring of equal opportunities data. No data processed by consent will be used in recruitment decision making.

We will only contact you with information about posts you may be interested in or other marketing related emails if you consent to receive this information. You may opt-out of these communications at any time.

Data is required for the following activities:

- To receive, administer, process, and communicate with you in relation to your enquiries, job alert subscriptions and/or applications.
- To administer marketing emails or to contact you in relation to roles we think you may be of interest to you.
- To assess your skills and qualifications for a particular job or task and make decisions about your requirement selection or appointment.
- To inform decisions to aid workforce planning and to facilitate the recruitment and selection process.
- To keep a record of our recruitment process
- To prepare employment contracts and agree terms of employment.

- To share with third parties engaged) for the consideration of relevant declared criminal convictions (DBS checks), Pre-Employment health or background checks, verifying your right to work in the UK and/or obtaining references.

- To ensure the safety and security of individuals and their property and the protection of university assets, including the use of CCTV, body worn cameras and ANPR images

- To enable anonymised reporting against Special Characteristics Data in line with our obligations under the Equality Act 2010

- To protect your vital interests, or those of another natural person, where you are physically or legally incapable of giving consent i.e., in an emergency, we may need to share information about any existing medial conditions.

- To enable statutory reporting to government bodies (e.g., the Higher Education Statistics Agency, Health and Safety Executive etc).

- To defend legal claims whenever courts are acting in their judicial capacity" or where there is a lawful requirement to disclose information to a third party.

- To assist police, local authorities, or other regulatory bodies for taxation purposes or pursuant to the prevention, detection, or disclosure of a potential crime.

- To comply with national Safeguarding protocols in the event of concerns for your safety or wellbeing and the wellbeing of others.

Please note that the above is not an exhaustive list and some of the above grounds for processing will overlap - there may be several grounds which justify our use of an Employee's personal information.

6. Personal Data may be shared with

We will make some statutory and routine disclosures of personal data to third parties where appropriate. These third parties include:

- Higher Education Statistics Agency (HESA)

- Higher Education Funding Council for England (HEFCE)

- UK Visas and Immigration, UK embassies, local authorities, and other government bodies, for the purpose of complying with our obligations to the Visa and Immigration Service

- The University Occupational Health Provider Pam Group where relevant to do so.

- Research sponsors/funders as per the funding agreements

- Former employers (where a reference is requested and with your consent) or educational establishments (to verify qualifications)

- Employment agencies engaged in the recruitment process you have engaged to act on your behalf.

- The police and other crime and fraud prevention and detection agencies, for crime prevention or detection purposes.

- Credit reference agencies or other background check agencies, where relevant

- To external lawyers, auditors, investigators, or insurers in respect of accidents occurring within the institution and where we need to seek advice and services in relation the "establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity" or where there is a lawful requirement to disclose information to a third party.

- TrustID who process digital identify services for right to work checks on behalf of the university.

- Atlantic Data who process DBS checks on behalf of the university where the role requires a DBS check.

If you are successful in your application, you may receive an offer subject to the completion of satisfactory employment checks and evidence of your right to work in the UK:

Criminal Convictions

We will only collect and share information about criminal convictions if it is appropriate given the nature of the role and where we are legally permitted to do so, e.g. the role requires a DBS check.

Right to work Eligibility Checks

We are required by law to conduct 'right to work' checks, for which we may share your personal information with TrustID, who are approved by the Government as an Identify Service Provider (IDSP) and undertake digital right to work checks on behalf of the University.

- Acuant, a sub-processor who on behalf of TrustID, use biometric data derived from 'selfie' or 'live capture' photographs for facial matching with right to work documentation provided in the right to work process.

Where applicable, you will receive an email offering you the chance to register and upload your details to TrustID, you will be required to upload a copy of your proof of right to work in the UK and a selfie. If you are not able to or choose not to provide proof of your right to work through TrustID, you will be required to arrange an appointment

with our HR team to carry out an in person right to work check, you must bring an original copy of your proof of right to work documentation to the appointment.

7. Transfers to third party countries

If you are applying from, or if your employment involves any period of study or employment outside of the European Economic Area (EEA) (known as 'Third Party Countries') we may transfer your data to support this.

Some of our partners, IT services or suppliers are also hosted by organisations either in third party countries, or who may back up their data to locations based in third party countries.

Where data is shared with third party countries, we ensure that these countries are either approved by the European Commission as having 'adequate protection' or we put in place 'appropriate safeguards' and contracts with these organisations, so as to maintain the security of the data and your rights under relevant Data Protection legislation.

There may also be limited sharing with organisation in third countries under specific exemptions, for example, with your explicit consent.

8. How personal data is stored securely by Northumbria University

We have implemented appropriate physical, technical, and organisational security measures designed to secure your personal data against accidental loss and unauthorised access, use, alteration, or disclosure. In addition, we limit access to personal data to those employees, agents, contractors, and other third parties that have a legitimate business need for such access.

All our employees, contractors, and volunteers with access to personal data receive mandatory data protection training and have a contractual responsibility to maintain confidentiality and access to your data is restricted to those members of staff who have a requirement to access it. Your data may be transferred and processed between relevant departments to provide you with access to services, to provide you with support or to fulfil the processing activities listed above.

We utilise many different storage solutions and IT systems, some of which are outsourced to third party providers. For example, email accounts are provided by the Microsoft Live@Edu service.

Where processing takes place with an external third party, processing takes place under an appropriate agreement outlining their responsibilities to ensure that processing is compliant with the Data Protection legislation and verified to be secure.

9. Automated individual decision making, including profiling.

We do not use "**Automated Decision Making**" (where systems make decisions about you 'automatically' without human intervention) or '**Profiling**' (where information about you is used to tailor goods or services based on your interests, movement, or records of your activities) for staff data.

10. How long personal data held by Northumbria University

You data is held in compliance with Human Resources section of Northumbria University's retention schedule, which is published on our website. This can be summarised as:

Unsuccessful applications will be retained for 6 months following appointment of the successful candidate, unless the position is filled by a candidate who requires sponsorship in which case minimum information will be retained in compliance with Home Office requirements.

The core record of your employment (dates of employment, role etc.) being retained for 80 years to process pensions and verify employment for future requests, and most records being held for 6 years beyond the end of your employment with us. Certain other records may be retained for differing period deepening upon legal requirement, for example 'asbestos legislation' etc.

11. Your Rights under GDPR

Under the GDPR, you have a number of rights in relation to the processing of your personal information, each of which may apply to differing degrees' dependent upon the nature of the processing and the legal basis for it. You have the right to:

- Be informed as to how we use your data (via this privacy notice)
- Request access (a copy) of the personal information that we hold about you.
- Correct inaccurate or incomplete data
- Request that we stop sending you direct marketing communications.

In certain circumstances, you may also have the right to:

- Ask to have certain data 'erased by us.
- Request that we restrict certain processing of your personal data.
- Request that we provide any data you submitted to us electronically be returned to you or passed to a third party as a data file.
- Object to certain processing of your personal data by us

In some cases, there may be specific exemptions as to why we aren't able to comply with some of the above. Where this is the case, we will explain the reasons why.

- For more information about any of the above please see the GDPR pages of our website.

- To exercise any of the above rights, please contact the Data Protection Officer (*details below*).

12. Data Protection Officer

The Data Protection Officer for Northumbria University is Duncan James.

Please do not hesitate to email us at dp.officer@northumbria.ac.uk. If your request is urgent, please call +44 (0)191 243 7357

13. Lodging a Complaint with the Information Commissioners Office (ICO)

If you are dissatisfied with our processing of your data, or a response to a complaint you have made to us about it, you have the right to complain to the ICO.

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Telephone: 0303 123 1113 (local rate) or 01625 545 745
Fax: 01625 524 510

For more information see Information Commissioner's web site.

14. Changes to this privacy notice

We keep this privacy notice under regular review and will communicate any significant updates to you. This privacy notice was last updated in September 2023 and will be reviewed annually.