Employee 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 an employee of Northumbria University, including Governors, self-employed or contracted personnel, temporary staff, or voluntary workers.

3. Where do we get your personal data from?

You provide data to us through an application or from third parties such as the Disclosure and Barring Service, background check providers or referees.

Data will be captured throughout your time as an employee, either from you through requests submitted to Human Resources, updates submitted through the staff portal, or via transactional activities as part of your employment and your engagement with university services and facilities.

We may also receive data from third parties such as pension scheme providers, HM Revenue and Customs, professional bodies or external partners and stakeholders.

4. Categories of personal data are processed by us.

To carry out our activities and obligations as an employer, we may collect, store, and process the following categories of personal data for the purpose of administering the employment relationship with you:

Data Category	Example
Contact	Name, title, addresses, telephone numbers, and personal email addresses
Biographical	Date of birth, gender, marital status and dependants, education, training, and employment history (places attended or worked), dates of study and examination results. National insurance number, nationality, country of domicile.
Administrative	Enquiry and correspondence records, application records (references, assessments, interview notes, offer letters), contracts, 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. Health and safety records* (assessments, accident reports).
Financial	Banking details, salary, benefits, pension scheme registration and administration, superannuation, and national insurance.
***Special category ("Sensitive") Personal Data**	Special Category data, including – racial or ethnic origin, age, disability, gender reassignment, marriage and civil partnership, religion or belief, sex, and sexual orientation. Relevant data relating to criminal convictions and offences. Trade union membership where required for planning and payroll purposes.
Performance and development	Personal development records, training records, professional memberships
Grievance or Disciplinary	Records of grievances, disputes, or disciplinary proceedings, including their investigations and outcomes
Photographs, audio, or visual recordings	Staff ID cards. Recording lectures, presentations, or workshops. Producing online profiles and departmental boards.
Security Data and Safety	Building entry, CCTV images, security incident reports and IT system login and usage.
Management planning	Workload and work allocations
Third Party	Marital and dependent status. Emergency contact information

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

Your personal data will only be processed for activities related to your employment or work activities, for example for staff management and workforce planning 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 to do wo (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.., processing unsolicited applications, shortlisting candidates etc.)

- Where required to carry out a task in the public interest (e.g., equal opportunities monitoring and reporting)

Under Article 6 EU GDPR we must identify a basis for the "Lawfulness of processing" of our activities involving of your data. These are broadly described as: 'Consent', 'Contract', 'Legal Obligation', 'Vital Interests', 'Public Interest (or Public Task)' and 'legitimate interests'.

Data is required for the following activities, which have been identified as necessary "for compliance with a legal obligation" under employment law, and "*for the performance of our employment contract with you"* or in the case of applicants, *"in order to take steps prior to entering into a contract*".

- Administration of your employment, including payroll, pension and benefits administration or other payments due under the contract of employment. Details of any payments your request us to set up via salary sacrifice (e.g., Childcare or Trade Union Membership).

- Assessing qualifications for a particular job or task, including decisions about promotions.

- Managing and monitoring sickness absence and other leave.

- Administering, monitoring, and supporting your personal development and training, including the provision of training delivered by third party providers.

- Providing access to, and managing your use of, University facilities and services, e.g., ID cards (including photographic image), building access, car parking, library membership and access to library systems, etc.

- Provision of access to IT systems and accounts, including registration with third party systems and hosting of data with third party providers. This may also include accessing email accounts and data during unexpected staff absence and post-employment (subject to formal authorisation and controls).

- Monitoring the use of university resources and undertaking investigations in line with relevant IT Policies.

- Provision of outsourced services provided by data processors on our behalf for any of the purposes for which we are permitted to process data in relation to your employment, including the provision of IT hosting, Academic partnerships, and other University services.

- Development of staff research profiles and the transfer of knowledge and intellectual property by associated University companies.

- Workforce planning, financial planning, and strategic forecasting, including statistical analysis for internal reporting and review and internal and external

auditing. Curriculum planning and organisation, timetable scheduling and any other associated planning.

- Administration of university codes of practices and policies, including, management of complaints, grievances, disciplinary and misconduct investigations.
- In relation to the safety and security of individuals and their property and the protection of university assets, including the use of CCTV.
- The operation of a lecture capture facility relating to the recording of teaching activities.
- Supporting your submission for Research Excellence Framework (REF) and Teaching Excellence Framework (TEF)
- For the recording of your termination of employment by voluntary resignation, redundancy, retirement (including on medical grounds) or dismissal.
- Staff contact details are publicly available via our contact directory and email directory. This you name, job title, work address, work email address and work telephone number.
- The dissemination of staff contacts details for use in connection with critical incident management plans. (e.g., personal contact details used to communicate with staff in times of emergency)
- Academic research records held in PURE profile will be used to publish your research profiles on our website.
- We will publish an academic or staff profile on the website as part of your employment to enable you to engage with relevant parties, but you will be asked to provide you explicit consent for the use of your images. You may additionally consent to your images being used in promotional material published on our website or in published brochures.

In addition to the lawful basis under Article 6, **Article 9** requires an additional condition for processing "**special categories"** (a.k.a "Sensitive") of personal data" relating to racial or ethnic origin, political opinions, religious or philosophical data concerning health or data concerning a natural person's sex life or orientation.

We recognise the significance of sensitive personal data and will only process such data if certain conditions are met. We may be required to process your sensitive personal data for the following purposes.

- Processing of Special Characteristics Data in line with our obligations under the Equality Act 2010

- Consideration of any relevant criminal convictions (DBS Checks) for employment purposes or any relevant matters that become known to us during your employment.

- 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 situation, we may need to share information about any existing medial conditions.

- Under employment law for compliance purposes such as equal opportunities monitoring, statutory reporting to government bodies (e.g. the Higher Education Statistics Agency, Health and Safety Executive etc) and internal compliance with relevant policies (e.g. Travel, Health and Safety etc)

- We will use information about the physical or mental health of an Employee, or their disability status, to ensure Employee health and safety in the workplace. This includes assessments of fitness to work, to undertake risk assessments and provide appropriate workplace adjustments, to monitor and manage sickness absence, and to administer benefits (statutory maternity pay, statutory sick pay, pensions, and permanent health insurance etc). We will also make appropriate referrals of staff to the external occupational health provider for the purposes of preventive or occupational medicine.

- Undertaking DSSR assessments, and the sharing of relevant information with “explicit consent” internally to enable reasonable adjustments to be facilitated.

- 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.

- Under relevant exemptions provided in the UK Data Protection Bill, processing may be required to assist police, local authorities, or other regulatory bodies for taxation purposes or pursuant to the prevention, detection, or disclosure of a potential crime.

- Under relevant exemptions provided in the UK Data Protection Bill, processing may be required in compliance with national Safeguarding protocols in the event of concerns for your safety or wellbeing and wellbeing of our students and others.

- Under relevant exemptions provided in the UK Data Protection Bill, processing may be required in compliance with national ‘PREVENT’ duties.

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.

Additional processing activities associated with your employment or your engagement with our services and facilities may be required, for example discussions at your request with your trade Union representative. We will endeavour to seek consent to

further process where applicable, unless processing is permitted under a relevant lawful basis.

6. Personal Data may be shared with

In addition to the above examples provider, we may make some statutory and routine disclosures of personal data to third parties where appropriate. These third parties include (but are not limited to):

- Higher Education Statistics Agency (HESA)
- Higher Education Funding Council for England (HEFCE)
- UK Visas and Immigration
- HM Revenue and Customs (HMRC)
- Your relevant Pension scheme – Teachers Pensions, TYPF, USS, UCRSS, NEST
- The University Occupational Health Provider
- Employer benefits provider
- Research sponsors/funders as per the funding agreement
- To the Office of the Independent Adjudicator where necessary to support their review of student complaints
- Disclosure and Barring Service (DBS)
- Atlantic Data who process DBS checks on behalf of the university where the role requires a DBS check.
- Mortgage lenders and letting agencies (where requested with your consent)
- Statutory Surveys Providers and other agencies conducting surveys on our behalf.
- Potential employers (where a reference is requested and with your consent).
- Responding to County Court Judgment (CCJ) requests
- Benefits Agency as required by the Social Security Administration Act 1992
- Child Support Agency as required by the Child Support Information Regulations 2008 (no.2551)
- Overseas tax authorities where staff are working overseas require us to do so
- Third party training providers you wish to
- Professional legal advisors or insurers acting on our behalf or on behalf of third parties.
- Placement providers, partners and employers where required as part of your employment. E.g., joint/collaborative course provision; staff exchanges. Apprenticeships
- Professional Bodies where necessary for accreditation purposes and/or the performance of your contractual duties
- Travel providers both nationally and internationally
- IT Service Providers contracted by us.
- Recognized trade unions to facilitate union membership and activity.

Any other disclosures that may be required but not listed above will be in accordance with your rights and the requirements of the GDPR.

7. Transfers to third party countries

Some of our partners, IT services or suppliers are also hosted by organisations either outside of the United Kingdom (UK), or who may back up data outside of the UK.

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, unless position is filled by a migrant worker in which case minimum information (CV or applications) 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 relationship 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.

If you would like to:

- Receive a copy of your data.
- Have any questions which you feel have not been covered by this Privacy Notice
- Have any concerns about the processing of your data
- Wish to make a complaint about the processing of your data

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.