

1. Introduction and Data Controller

The University of Northumbria at Newcastle (“we”, “our”, “us”) is registered with the Information Commissioners Office as a Data Controller - Registration Number [Z7674926](#). We are committed to processing personal data in accordance with our obligations under the General Data Protection Regulation (GDPR), the Data Protection Act 2018 and any related UK data protection legislation.

This privacy notice describes how and why we process personal data in relation to individuals (“you”, “your”) involved in a financial transaction with us and explains how you can control the processing of your data or exercise your rights under the GDPR.

2. Where do we get your personal data from?

You may give us your personal data through your relationship with us (such as through application or enrolment), when you make an enquiry to us, or when you instigate a financial transaction with us (for example you make a payment to us) or when we instigate a transaction with you (for example we make a payment to you). We may also receive your personal data from a third party acting on your behalf to administer a financial transaction.

3. Categories of personal data we process

To carry out our activities and to manage our relationship with you, we may process the following categories of data:

Customer account identifier information such as name, relevant identity numbers (Student Number, Customer Number, National Insurance Number), Date of Birth, Signature, IP address.
Customer contact information such as your (home/billing or work) address, phone number, email or other online identifiers.
Funding and financial information including bank details, sponsors, scholarships.
Bank card information including name on credit or debit card, card type, card expiry date, and the first six and last four digits of your card number.
Payment transaction details, including payment amounts and frequencies, dates of payments, payment plans, status of payments, including late payments... Payment descriptions and gateway transaction ID. Any other reference numbers.
Records of the nature of the interactions such as event and merchandise sales and purchases, and any related information.
Detail of complaints or disputes.
Feedback from you.
Supplier and contractor information including names, contact details, communications with contractors contracts, tender information, works undertaken, items purchased, invoicing arrangements, VAT numbers and payments made, banking details, information about the selection of contractors/suppliers, including information about the quality and/or value of the work or products.
Special Category Data relating to your health and disabilities may be required for some transactions such as to claim appropriate taxation allowances or support claims.

4. The lawful basis for processing your data

The first principle of the General Data Protection Regulation (GDPR) requires that whenever an organisation processes personal data, it must be processed 'lawfully, fairly and in a transparent manner'. This requires us to identify a lawful basis under Article 6 GDPR and Article 9 GDPR for special Category Data such as:

Article	Description
6(1)(a)	With your consent to process your data, for example if you engage with a specific service. Where we rely on consent this will be made clear to you and you are free to decide whether to provide this data with no consequences if you choose not to.
6(1)(b)	Processing is necessary for the performance of our contract with you as a registered student (or in order to enter into a contract). Without this information we would not be able to process your data to provide the contracted services or provide the support necessary to fulfil that contract.
6(1)(c)	Some processing is necessary to because we have a Legal obligation to do so, for example for the prevention and detection of crime or fulfil our statutory compliance and regulatory obligations.
6(1)(e)	Where "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller"
9(2)(a)	With your explicit consent to process special category data your data. Where we rely on you are free to decide whether to provide this data. There will be no consequences if you choose not to and you may later withdraw consent.
9(2)(f)	Where processing is necessary in relation to legal claims.
9(2)(g)	We may need to process special category data if the processing is necessary in the substantial public interest and there is a basis to do so in law
9(2)(j)	We may process special category data for archiving, scientific or historical research purposes or statistical purposes, where there is a basis to do so in law

5. Why do we process your Personal Data?

We process personal data in order to administer our financial activities, manage our finances and protect against fraudulent activities. To do this we process data for the following purposes:

Activity	Legal Basis
Maintaining accurate and up to date customer and supplier account records.	6(1)(b)
Administer the collection of fees owed to the University, and to make payments and repayments.	6(1)(b) & 6(1)(c)
Administer student expense claims.	6(1)(b) & 6(1)(c)
Process complaints	6(1)(b), 6(1)(c) & 6(1)(e)
To detect, investigate and prevent crime including fraud	6(1)(b), 6(1)(c) & 6(1)(e)
To process insurance claims which may include disclosure of sensitive personal data	6(1)(a) & 9(2)(a); or 6(1)(b), 6(1)(c), 6(1)(e) or
To meet legislative, statutory, contractual and audit requirements	6(1)(b) & 6(1)(c)
To maintain or develop our systems, to monitor and improve our processes and improve our services.	6(1)(e)

Finance Privacy Notice

For research and statistical purposes and to respond to requests for information under relevant legislation.	6(1)(c), 6(1)(e), 9(2)(g), & 9(2)(j)
--	--------------------------------------

6. Sharing your Personal Data with Third Parties

We may disclose certain personal data to external bodies, as categorised in the table below, only where we have a legal basis to do so in accordance with UK data protection law.

Transfer To	Purpose
Student Loans Company (Privacy Notice) and other funding bodies including NHS Business Services Authority.	For verification of your enrolment and the contractual administration of your payments
Sponsors and private funding bodies including employers and overseas bodies.	In accordance with the terms of their contract with you, or with your consent, we will confirm periods of attendance, assessment results and similar information.
HMRC	To verify details or to provide information in relation to payments made
Financial Institutions including Banks, Building Societies, BACS, Brokers, Payment Gateways and other related payment processing services such as WPM Education and Western Union.	For processing contractual financial transactions.
Government agencies and authorities with official duties for the apprehension and prosecution of offenders, collection of a tax or duty, or safeguarding national security	Where it is permitted under UK law in order to assist the requesting body fulfil their statutory duties.
Companies acting as 'data processors' under contract to the University.	The University may engage external companies to deliver functions on our behalf, for example cloud storage analytical services. They will only process data for the purpose for which we have engaged them and will not process your data in any other manner.
External solicitors, brokers or insurers in respect of potential claims against the institution.	Where we need to seek advice and services in relation to the "establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity".
External parties such as solicitors, debt recovery agents, tribunals and Courts.	Where internal University procedures have failed to recover outstanding debts.
To External Auditors	To allow them to review compliance with regulations and to ensure our effective operations.
Any other disclosures that may be required but not listed above will be in accordance with your rights and the requirements of the UK Law.	

7. How do we keep your Personal Data Secure?

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.

We utilise many different storage solutions and IT systems, some of which are outsourced to third party providers. 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

All 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.

Where applicable, any credit/debit card details provided will be stored in full compliance with PCI-DSS requirements.

8. Transfers to countries outside of the European Economic Area (EEA)

Some Partner and IT services providers are based in countries outside of the EEA. The university will only transfer data to outside the EEA where satisfied that both the party which handles the data and the country it is processing it in provide adequate safeguards for personal privacy. 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 ensure that we have 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.

9. How Long will your Personal Data Held?

We will retain your personal data for as long as it is required to fulfil the purpose for which is it held and then to fulfil any legal requirements. Details of the retention periods for each type of processing activity is detailed in our retention schedule which is available on our [Finance Retention Schedule](#)

10. What Are Your Rights Under GDPR?

GDPR provides individuals a number of rights in relation to the processing of personal data, 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

11. Data Protection Officer (DPO) Contact Details

Our Data Protection officer is Duncan James. To exercise your rights, or if you wish to raise a concern about our processing of your data, please contact the DPO on +44 (0)191 243 7357 or via email at dp.officer@northumbria.ac.uk.

12. 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, you have the right to complain to the ICO via Telephone: 0303 123 1113 (local rate) or 01625 545 745, via email: casework@ico.org.uk or for more information see [Information Commissioner's web site](#).