



CONTRACTORS AND CONSULTANTS PRIVACY NOTICE

Who we are?

We are the University of Northampton and we process your personal data to provide you with University services, to undertake our responsibilities and legal/statutory obligations, and to monitor our own performance.

The University of Northampton is a data controller, registered with the Information Commissioner's Office, and for the purposes of the Data Protection Act 2018 and the General Data Protection Regulation (GDPR), we have appointed a Data Protection Officer who has formal responsibility for data protection compliance within the organisation.

Our Data Protection Officer is Phil Oakman and he can be contacted at:

Recordsmanager@northampton.ac.uk

Or by writing to: Records Management Office, University of Northampton
(Waterside Campus), University Drive, Northampton NN1 5PH

What data do we hold about you?

The type of data the University of Northampton holds about you is that which is necessary to carry out our business relationship.

Data held about you may include, but is not restricted to, the following:

- Personal details such as name, date of birth, emergency contact details, and National Insurance number
- Bank or building society account details
- Records concerning Performance Development Review and training
- Qualification details
- Contracts
- Correspondence between you as consultant/contractor and the University

- Health and safety records (including accident reports)
- Occupational Health Information
- Your use of UON facilities such as the library
- Disclosure and Barring Service (DBS) checks (required for select positions)

How do we collect your data?

Direct Collection

We collect data to operate effectively and provide you the best experience at this University. You may provide some of this data directly to us, from forms you complete or identity documents you provide at the start of, or during the course of your work with us. It is your responsibility as the contractor or consultant to ensure that the data we hold about you is accurate and up to date.

In-direct Collection

We may also occasionally obtain data from third parties, for example a consultancy agent or HMRC.

Why do we process your data?

We may process your personal data because it is necessary for the performance of a contract with you. For example, to pay you in accordance with the contract.

We may also process your personal data because it is necessary for the performance of our tasks carried out in the public interest or because it is necessary for ours, yours or a third party's legitimate interests. In this respect, we may use your personal data for example for the following:

- to monitor and evaluate the performance and effectiveness of the university;
- to maintain and improve the academic, corporate, financial, estate and human resource management of the university;
- to promote equality and diversity throughout the university;
- to seek advice on our rights and obligations, such as where we require legal advice;
- recovering money if owe to us;
- to pay you money as part of a contractual agreement.

In other cases the University has a legitimate interest in processing personal data before, during and after the end of the relationship in order to:

- Obtain occupational health advice to ensure it complies with duties in relation to individuals with disabilities and meet its obligations under health and safety law
- Ensure effective administration
- Respond to and defend against legal claims

- Provide facilities such as IT, Library and car parking

We may also process your personal data for our compliance with our legal obligations. In this respect, we may use your personal data for the following:

- to meet our compliance and regulatory obligations, such as compliance with anti-money laundering laws and safeguarding requirements;
- for the prevention and detection of crime;
- in order to assist with investigations (including criminal investigations) carried out by the police and other competent authorities.

We may also process your personal data where:

- it is necessary for medical purposes
- it is necessary to protect your or another person's vital interests; or
- we have your specific or, where necessary, explicit consent to do so.

Who has access to the data?

Your information may be shared internally, such as with members of the HR and payroll teams, your line manager, senior managers in the area in which you work and the University executive team and IT staff, but only if access to the data is necessary for the performance of their roles.

The University may share data with other organisations as necessary and to fulfil our statutory obligations as an employer. At all times the information shared and the manner of disclosure will be in accordance with the provisions of the Data Protection Act. Below are some of the organisations we share with but this is not an exhaustive list:

- HESA (Higher Education Statistics Agency) – in anonymised format
- HMRC (Her Majesty's Revenue and Customs) – for the administration of tax and National Insurance
- The University's occupational health provider – for the provision of occupational health and wellbeing services
- Other public authorities or public partnerships, such as schools, hospitals, police as the law requires.
- Non-commercial organisations that may also help with service delivery
- Business we hold contracts with to help deliver our services to you
- Disclosure and Barring Service (DBS) via an intermediary company, GBG, (required for select positions)
- Internal or External auditors - for checking the integrity of our data and processes

How do we keep your data secure?

The University takes the security of your data seriously. The University has internal policies

and controls in place to ensure that your data is not lost, accidentally destroyed, misused or disclosed and is not accessed except by its employees in the performance of their duties. Where the University engages third parties to process personal data on its behalf, it does so on the basis of written agreement. The third parties are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

We will keep your personal data only as long as is necessary to conclude the purpose(s) for which it was collected and in accordance with the University's Record Retention Schedules which can be found [here](#).

Data will be securely destroyed when no longer required.

Your rights

As a data subject you have a number of rights. You can;

- Access and obtain a copy of your data on request
- Require the university to amend incorrect or incomplete data
- Require the university to stop processing your data, for example where the data is no longer necessary for the purposes of processing
- Object to the processing of your data where the university is relying on its legitimate interests as the legal ground for processing
- require us to erase your personal data;
- require us to restrict our data processing activities (and, where our processing is based on your consent, you may withdraw that consent, without affecting the lawfulness of our processing based on consent before its withdrawal);
- receive from us the personal data we hold about you which you have provided to us, in a reasonable format specified by you, including for the purpose of you transmitting that personal data to another data controller;

Please note that the above rights are not absolute, and we may be entitled to refuse requests where exceptions apply.

If you wish to exercise any of these rights or if you have a complaint about the way you believe your data is being processed, in the first instance, discuss this with the records management team by emailing: recordsmanager@northampton.ac.uk

If you have a complaint and you remain dissatisfied with how your complaint has been dealt with you can take your complaint to the Information Commissioner's Office (ICO) for a review.

<https://ico.org.uk/>