

1. Data Controller

University of Northumbria at Newcastle processes personal data in accordance with our obligations under the General Data Protection Regulations ('GDPR') and is a registered Data Controller with the Information Commissioner's Office ('ICO'), which is the supervisory authority responsible for the oversight and enforcement of Data Protection Legislation within the United Kingdom.

Data Controller: University of Northumbria at Newcastle
Registration Number: Z7674926

2. Overview

For the 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. This privacy notice is a statement that describes how and why the Student Law Office ("we", "our", "us") processes personal information in relation to the services provided to any individual ("you", "your") making enquiries about or making use of our services.

This notice also explains how you might control the use of your personal data in accordance with your rights under the GDPR. You may be given further information about the uses of personal data when accessing specific services and facilities.

3. Where do we get your personal data from?

You provide data to us when you make an enquiry and during the course of us providing our services to you. This may be through your use of our website when you contact us, via telephone, email or written correspondence when you engage our legal services or as a result of your relationship with our staff.

We may additionally obtain information from third party sources in the course of providing legal services. In this instance we will always try to ensure that the third party has lawful authority to provide us with your personal data.

4. Categories of personal data processed by the University

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

- **Identity information** - your name (including prefix or title), your title or position, age, gender, nationality, date of birth, national insurance number, country of domicile and your relationship to a person. This may include details of your spouse/partner and dependants or other family members.
- **Contact information** - your postal address, email address and phone number(s).
- **Enquiry information** - the information you provide to us, by telephone, in writing, email or through our online enquiry form, for the purposes of enquiring

about our services in the SLO. We collect notes from our conversations with you when you make a telephone enquiry and during meetings with you whether by telephone, virtually or face to face.

- **Identification and background information** provided by you or collected as part of our procedures for engaging you as a client of the SLO, for example we may need to take a copy of your passport, driver's license or a utility bill.
- **Financial information** collected or generated by us in the course of providing legal services such as banking details, hardship, records of payments, salary, benefits, pension, national insurance and other necessary information. We may require financial information relating to family or personal circumstances and supporting evidence.
- **Service and regulatory information** provided to us by you or someone on your behalf, or generated by us in the course of providing legal services. This may include **Special Category Data**. For example to comply with our regulatory requirements we process documents you provide to prove your identity such as a passport or driver's licence.
- **Special Category Data** may be held by the SLO if the nature of our initial enquiry work and retainer implies a need for such information. Special Category Data means personal information revealing racial or ethnic origins, political opinions, religious beliefs, philosophical beliefs or trade union membership; genetic and biometric data; data concerning health, sex life or sexual orientation. This also includes relevant data relating to criminal convictions and offences.
- **Personal Data of children** if your enquiry or the services we provide to you involves children, these children must be represented by their parents or guardians. In these circumstances we will explain to the parent or guardian why we need any personal information relating to the children and how it will be used, both when we first collect the data and during the course of our services.
- Any other information relating to you which you may provide to us.

When you provide personal information to us relating to a third party you confirm that you have any necessary permission or authority to do so. You are also responsible for ensuring that the provision of that personal information complies with data protection and other applicable law.

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

Under **Article 6** EU GDPR we must identify a basis for the "Lawfulness of processing" of our activities involving 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 the following activities which have been identified as necessary "for the performance of our contract with you".

- The administration of students' studies, academic assessment and progression in the SLO. Including the administration of student related policies and procedures for example complaints and conduct.
- To receive, consider and progress your enquiry for the provision of legal services by us to you.
- To provide legal services to you and comply with our regulatory requirements.
- For the processing and recovery of accounts and fees incurred in the course of providing legal services to you.

These further activities have been identified as processing where it is “necessary for the purposes of the legitimate interests pursued by the controller” (us) or, where as an enquirer or client, you have “given consent to the processing of personal data for one or more specific purposes”. You can withdraw consent for, or object to processing, for these purposes at any time.

- When you make an enquiry for legal services by telephone, online, in writing or by email.
- When we first contact you to progress your enquiry. At this stage we may ask you to provide further information to help with our assessment of your enquiry and attend an interview which will be recorded with your consent.
- To comply with our legal and regulatory requirements as a provider of legal services.
- To analyse, monitor, maintain and enhance the quality of our staff and services.
- Development of staff research.
- The operation of a video capture facility to record our meetings with you.
- For the production of statistical returns required for third party bodies such as Lawworks.
- Gathering and providing information required by or relating to audits, enquiries or investigations by regulatory bodies.
- Ensuring our policies are adhered to.
- Preventing unauthorised access and modifications to systems.
- Updating and maintaining client records.
- For education, training and development activities including research and statistical analysis for internal reporting and review for financial and strategic planning.
- Administration and delivery of legal services including the processing and recovery of accounts and fees.
- Provision of information to external examiners for academic assessment.

In addition to the lawful basis under Article 6, **Article 9** requires an additional condition for processing Special Category personal data (“Sensitive”) 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.

There may be circumstances where processing is necessary.

- For the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
- Where there are reasons of substantial public interest, on the basis of UK Law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.
- We may be required to process your Sensitive data to protect your vital interests or those of another natural person where you are physically or legally incapable of giving consent.
- To external lawyers, auditors or insurers 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” or where there is a lawful requirement to disclose information to a third party.
- Under UK Law 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 UK Law, processing may be required in compliance with national Safeguarding protocols in the event of concerns for the safety and wellbeing of you, our students and others.
- Under UK Law, processing may be required in compliance with regulatory obligations, such as compliance with anti-money laundering laws and safeguarding requirements.

Please note the above is not an exhaustive list. Additional processing activities associated with your engagement with us may be required in the event of requests made by an outside agency or as a result of activities undertaken as part of our relationship with you.

We will endeavour to seek consent to further processing where applicable, otherwise processing will only occur where an additional lawful basis can be found.

6. 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. Access to your personal information is restricted to those members of staff and students who have a requirement to maintain a relationship with you or provide legal services to you. Such access is controlled through user security profiles, an electronic data secure server and key pass entry and exit to the SLO.

For the purposes of assessment and meeting our regulatory requirements we may need to provide access to your personal information to third parties.

All of our employees and contractors 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.

The University utilises 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.

Your client file is stored on our Case Management System (CMS). This is a secure data centre in the UK. We have outsourced the provision and maintenance our CMS to a third party provider who acts as a data processor under the control of the University. This third party provider processes personal data following our review of their capacity to securely store personal data and under an appropriate agreement outlining their responsibility to ensure that processing is compliant with Data Protection Legislation. Our third party provider is accredited with the CyberSafe Essential's certificate and has adopted the standards and ensures data is stored and processed in line with ISO 27001.

7. Sharing your Personal Data with Third Parties

We need to share your personal information with third parties such as:

- External moderators for the purpose of academic assessment
- The Solicitors Regulatory Authority for the purpose of regulating how we deliver our legal services
- Other providers of legal services for the purpose of providing legal services to you
- The Legal Ombudsmen for handling complaints
- Third parties acting as “data processors” under the control of the University.
- The University may engage external companies to deliver functions on our behalf, for example cloud storage for our case management system. They will only process data for the purposes for which we have engaged them and will not process your data in any other manner.

On occasion the University may also be obliged to provide information to the Police, Local Authorities, other Relevant Government Departments or other third parties if it is necessary under an appropriate exemption provided by the legislation. We will only do this after full consideration of your rights and the correct application of such exemptions.

8. Transfers to third party countries

Some of our IT services or providers are hosted by organisations 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.

9. How long personal data held by Northumbria University

We will only retain your personal data for as long as necessary to fulfil the purposes for which we collected it. This includes satisfying any legal, regulatory or reporting requirements.

To determine the appropriate retention period for personal data, we consider the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

At the end of the retention period, your data will be either deleted completely or anonymised so it can be used in a non-identifiable way for statistical analysis, business and educational planning.

Type of Data	Description	Maximum Retention Period	Criteria
Enquiry Data	Expressions of interest in the services of the student law office	12 months	To allow for assessment, business and educational planning
Initial Client Interview Data	To assess your enquiry including a recorded interview	12 months	To allow for assessment, business and educational planning
Client Data	To provide legal services	6 years from the date we end our contractual relationship with you. For miscarriage of justice cases the maximum	For the purpose of risk management and responding to claims and complaints

		retention period will be for the period of the sentence plus six years	
Student Assessment Data	To assess students' personal folders submitted and retained for assessment and moderation	Up to the 30 September being the September immediately following your enquiry. This means your data will be held for this purpose for a maximum of 12 months	To allow student assessment and moderation

10. 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.

All communication with you, including in relation to updates to this privacy notice, will be made via the preferred method of communication that you have registered with us, and you will be able to select the type of correspondence you receive.

If, at any stage, you are concerned about the content (e.g. unwanted marketing), frequency (too many) or method (change preference) of these communications, you can unsubscribe or update your preferences using the link which will be provided at the bottom of the relevant correspondence.

Please note that the option to unsubscribe may not be included in direct personal correspondence with individual members of staff, but you may request to them that you be removed from our systems.

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

- Ask to have your data 'erased by us.
- Request that we restrict the processing of your personal data.
- Request that we provide any data you submitted to use electronically be returned to your 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](#).
- In order to exercise any of the above rights, please contact the Data Protection Officer (*details below*).

11. Data Protection Officer

The Data Protection Officer (DPO) for Northumbria University is Duncan James. Contact the DPO if you would like to:

- Receive a copy of your data.
- Have any questions 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

You can email at dp.officer@northumbria.ac.uk or call +44 (0)191 243 7357

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 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

For more information see [Information Commissioner's web site](#).

13. 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 2021 and will be reviewed annually.