Employee Privacy Notice

Data Controller: Norwich University of the Arts

As part of any recruitment process, Norwich University of the Arts collects and processes personal data relating to job applicants. The University is committed to being transparent about how it collects and uses that data and to meeting its obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA).

If you are a member of staff who is also a student or alumnus of the University, please also see our Student and Alumni Privacy Notices.

What information the University collects

The University collects and processes a range of information about you. This includes:

- your name, address and contact details, including email address and telephone number, date of birth and gender;
- Images. For example in the production of ID cards;
- the terms and conditions of your employment;
- correspondence between you and the University;
- correspondence between the University and third parties on your behalf, for example a mortgage lender or letting agency;
- details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the University;
- information about your remuneration, including entitlement to benefits such as pensions;
- details of your bank account and national insurance number;
- information about your marital status and emergency contacts;
- details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence; and
- assessments of your performance, including probation reviews and appraisals, training you have participated in, performance improvement plans and related correspondence.

The University may also collect and process ‘sensitive personal data’ under the DPA, and ‘special categories of data’ under the UK GDPR including:

- information about your nationality and entitlement to work in the UK;
- details of your working pattern and attendance at work;
- details of periods of leave taken by you, including holiday, sickness absence, family leave and other, and the reasons for the leave;
- information about medical or health conditions, including whether you have a disability for which the University needs to make reasonable adjustments;
- health and safety records (including accident reports) and security (including University-operated CCTV;

- information about trade union membership; and
- equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief.

For some roles, the University is also obliged to seek and process information about criminal convictions and offences.

How and why we collect this information

The University collects this information in a variety of ways. For example, data is collected through application forms, CVs; obtained from your passport or other identity documents such as your driving licence; from forms completed by you at the start of or during employment; from correspondence with you; or through interviews, meetings or other assessments.

In some cases, the University collects personal data about you from third parties, such as references supplied by former employers and information from criminal records checks where this is required for the specific role.

We collect personal information from you for a range of purposes. The University complies with the provisions of the Data Protection Act 2018 which sits alongside the UK General Data Protection Regulation (UK GDPR). Article 6 of the UK GDPR defines six different lawful grounds for an organisation to be permitted to process personal data, and the University is legally obliged to determine and advise you of under which of the legal bases the different categories of your personal data is processed, although, in some cases, more than one of these may apply. These are as follows:

The University needs to process data on entering any contract with you and relies on Article 6(1)(b), '*for the performance of a contract (or negotiations entering into a contract)*' as its legal basis for doing so. Processing in performance of your contract enables us to undertake the administration of the terms and conditions of your employment, such as paying you, monitoring your training, performance, and workload, and managing your benefits and pension entitlements.

The University will rely on Article 6(1)(c) *'legal obligation'* when processing of your personal data is absolutely necessary for the University to comply with a legal obligation. As an example, it is a legal requirement that we check an employee's entitlement to work in the UK, to comply with Home Office and tax obligations, to comply with health and safety laws, to obtain occupational health advice to ensure we meet our obligations, and to enable employees to take periods of leave to which they are entitled. This also includes our legal obligations to comply with Data Protection and Freedom of Information legislation.

The University will rely on Article 6(1)(a) *'consent'* where you have given clear consent for us to process your personal data for a specific purpose. Examples of this are where you have provided this data for the purposes of joining a pension scheme or where you have elected to be notified of services and events relating to your employment. Where we rely on consent as our legal basis, it should be noted that you have the right to withdraw this consent at any time, as detailed later in this Notice.

The University may rely on Article 6(1)(d) *'vital interests'* to use your personal data in the event of a life-threatening medical emergency.
The University will rely on Article 6(1)(e) *'public task'* where the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law. This would apply where we are using your personal data to enable you to undertake your role in the University.

The University will rely on Article 6(1)(f), '*legitimate interests*' as its legal basis where we judge the use of the personal data to be within our legitimate interests. We have given consideration as to whether those interests are overridden by the rights and freedoms of employees or workers and conclude that they are not, as processing data from employees allows the University to:

- maintain accurate employment records and contact details (including emergency contact details), and records of employees' contractual and statutory rights;
- operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace;
- ensure strong general HR and business administration practices to enable effective and robust workplace management;
- review staff opinions and ideas through surveys;
- monitor individual access and use of specific facilities and premises where we believe this to be in the interests of safety or to protect our property;
- ensure insurance provision, for example, travel insurance;
- participate in benchmarking, surveys and data sharing with professional bodies;
- provide you with access to training and development services;
- provide confidential counselling, advice, coaching or support services;
- provide references on request for current or former employees;
- respond to and defend against legal claims; and
- maintain and promote equality in the workplace by producing statistics to analyse changes in our staff population and ensure that our policies and practices do not disadvantage minority groups.

Some of the personal information collected, held, and processed will be classed as 'sensitive personal data' also known as 'special category personal data.' Where the University processes special categories of data, such as information about ethnic origin, sexual orientation, health, or religion or belief, this is for equal opportunities monitoring purposes
in relation to the Equality Act 2010.

The University also processes special category personal data about health or medical conditions to satisfy its employment law obligations (such as those in relation to employees with disabilities and for health and safety purposes). Information about trade union membership is also considered as special category personal data and this is processed to allow the University to operate check-off for union subscriptions.

Access to and the sharing of this kind of 'special category' personal information is strictly controlled. The University's legal bases for processing this sensitive data under Article 6 of the UK GDPR are Article 6(1)(e), '*for the performance of a public task in the public interest' and* Article 6(1)(f), '*legitimate interests*'. In addition, for sensitive data, the University is required to identify an appropriate lawful condition under Article 9 of the UK GDPR which is Article 9(2)*(a) 'explicit consent',* Article 9(2)*(b) 'employment' and* Article 9(2)*(g) 'substantial public interest'.*

For some roles, the University is obliged to seek and process information about criminal convictions and offences. Where the University seeks and processes this information, it does so under Paragraph 1 of Schedule 1 of the Data Protection Act 2018 because it is necessary for it to undertake its obligations and exercise specific rights in relation to employment.

How we use your information

The University will use your data only for the purposes relating to your employment, as detailed in the section above. Data is stored in a range of different places, including in your personnel file, in the University's HR management systems and in other IT systems including email. The University takes the security of your data seriously. It 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 our employees in the proper performance of their duties. There may be circumstances where your data is processed on systems which are hosted outside of the UK. Where this is the case, the University ensures that these organisations have safeguards in place, which meet the appropriate standards required to protect your personal data.

Automated Decision Making and Profiling

As part of our commitment to protecting your personal data, we want to inform you that the University currently limits the use of automated decision-making and profiling in line with the requirements of the UK GDPR. However, as we continue to develop our services, there may be instances in the future where automated processes are used to make decisions or create profiles. Should this occur, we will ensure that appropriate safeguards are in place and will always ensure that human intervention is involved when decisions are made that impact you.

Who we might share your information with

Your information will be shared internally, including with members of the HR team (including payroll), your line manager, managers in the area in which you work and IT staff if access to the data is necessary for performance of their roles.

The University shares your data with third parties in order to obtain pre-employment references from other employers, obtain necessary criminal records checks from the Disclosure and Barring Service (if required for the role) and the Home Office, UK Visa and Immigration to meet the obligations as a visa sponsor.

The University also shares your data with third parties that process data on its behalf, in connection with payroll, the provision of benefits, the occupational pension scheme and the provision of occupational health services.

Your information may be shared with the providers of any external/collaborative learning and training to give you access to third-party training and development services.

We may disclosure personal information to external bodies to fulfil our statutory and contractual responsibilities. Anonymised data is shared with the Higher Education Statistics Agency (HESA) for statistical analysis. It is important to note that, with effect from 4 October 2022, any personal data processed by HESA as controller has been transferred to Jisc, who is now the data controller of this personal information. This means that Jisc determines the manner and purpose of its use. You can find further details by reading their updated Privacy Notice here.

How long we keep your information

The University will hold your personal data for the duration of your employment and for a further period thereafter of six years. After this period, it will ordinarily be destroyed, in line with the University's data retention schedule.

International Data Transfers

We may transfer your personal data to countries outside the UK (third countries), including countries within the European Economic Area (EEA) and beyond, where our third-party service providers or affiliated organizations are based. Such transfers may involve countries that do not have data protection laws equivalent to those in the UK.

When transferring personal data to a third country, we take steps to ensure that your data is protected in line with the UK General Data Protection Regulation (UK GDPR). These measures include the use of the following safeguards, where appropriate:

1. **Standard Contractual Clauses (SCCs)**: For transfers to third countries that do not provide an adequate level of data protection, we implement the European Commission's Standard Contractual Clauses (SCCs) or equivalent contractual mechanisms as approved by the UK Information Commissioner's Office (ICO). These clauses legally bind the recipient of the personal data to ensure that your data is processed in accordance with the standards set out by the UK GDPR.

2. **Adequacy Decisions**: Where applicable, we may transfer your personal data to a third country that has been recognised by the UK government as providing an adequate level of data protection. In such cases, no further safeguards are required, and the transfer will be made in compliance with the UK's adequacy regulations.
3. **Additional Safeguards**: In some cases, additional measures may be taken, such as encryption, pseudonymisation, or other technical and organisational safeguards, to further protect your personal data during the transfer process.
4. **Transfers to Internal Organizations**: Your personal data may also be transferred to other entities within our university group or related organizations, including those based outside the UK, to support internal administrative functions, academic services, or research purposes. Any such transfers will be governed by appropriate safeguards, including but not limited to SCCs or other legally recognised measures under the UK GDPR.

We will ensure that any data transfer to third countries is carried out with appropriate legal protections in place, and we will provide you with further information upon request regarding the specific safeguards applied in relation to your data.

Your rights

Under data protection law, you have rights including:

- Your right of access - You have the right to ask us for copies of your personal information (this is known as a Subject Access Request or SAR).
- Your right to rectification - You have the right to ask us to rectify personal information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.
- Your right to erasure - You have the right to ask us to erase your personal information in certain circumstances.
- Your right to restriction of processing - You have the right to ask us to restrict the processing of your personal information in certain circumstances.
- Your right to object to processing - You have the right to object to the processing of your personal information in certain circumstances.
- Your right to data portability - You have the right to ask that we transfer the personal information you gave us to another organisation, or to you, in certain circumstances.

You are not required to pay any charge for exercising your rights. If you make a request, we have one month to respond to you.

It is important to note that some of these rights are not absolute and will depend on the circumstances. Please contact our Data Protection Officer at dataprotection@norwichuni.ac.uk if you wish to make a request or have any queries.

The Information Commissioners website provides more information on data rights.

What if you do not provide personal data?

Information, such as contact details, evidence of your right to work in the UK, and bank details must be provided to enable the University to enter a contract of employment with you. You also have obligations under your employment contract to provide the University with certain data. For example, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith. You may be required to provide the University with data in order to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide this data may mean that you are unable to exercise your statutory rights.

Failure to provide any information which the University requests, in its capacity as your employer, may hinder its ability to efficiently manage the rights and obligations which are a necessary part of an employment relationship.

How to contact us

If you require further information or have any concerns about how your personal information is held and processed by us, please email the University's Data Protection Officer (Chris Dubinski) at dataprotection@norwichuni.ac.uk or write to us at Data Protection Officer, Norwich University of the Arts, Francis House, 3 -7 Redwell St, Norwich NR2 4SN.

You can also complain to the ICO if you are unhappy with how we have used your data.
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

ICO Helpline number: 0303 123 1113
ICO website: https://www.ico.org.uk

Changes to this privacy notice

We keep our privacy notices under regular review.

This privacy notice was last updated on April 2025.