Privacy Notice for Employees and Other Workers

Privacy Statement

The General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (and, where applicable, EU GDPR) govern the way organisations use personal data. Personal data is information relating to an identifiable living individual. Transparency is a key element of GDPR, and this Privacy Notice is designed to inform Employees and Other Workers about how and why the University uses your personal data, what your rights are under GDPR, and how to contact us so that you can exercise those rights.

Data Protection Principles

We will comply with data protection law and principles, which means that your data will be:

- Used lawfully, fairly, and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept securely.

Who Are We

The University of Suffolk is an institution dedicated to transformation – transforming individuals, our community, our region, and beyond. Education, training, and research are powerful tools to support transformation and change, and to fulfil these obligations, the University collects, stores, processes, and shares personal data.

This privacy notice makes you aware of how and why your personal data will be used, as a prospective, current or former employee of the University of Suffolk, as a volunteer, consultant or contractor of the University of Suffolk, and how long it will usually be retained for. The University of Suffolk is a “data controller”, which means we are responsible for deciding how we hold and use personal information about you.

Lawful Basis for Using the Data

Our lawful basis for using the data includes:

- Necessary for the performance of a contract.
- Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- Necessary so we can comply with our legal obligations as your employer.
- Necessary to protect your vital interests or those of another person.
- Necessary for the purposes of our legitimate interest.

Personal Data We Collect

We will process personal data about you to meet our responsibilities as an employer and to manage our relationship with you as a University of Suffolk employee, casual worker, volunteer, consultant, and contractor. This may include:

1. Personal Identification and Contact Details:
- Name (first, last, and any previous names)
- Title
- Home address
- Personal and work email addresses
- Telephone numbers (home, work, mobile)
- Date of birth
- Gender
- National Insurance number
- Photograph for an ID card

2. Employment Details:
- Job title and role descriptions
- Employment history and previous employers
- Start and end dates of employment
- Contractual terms (e.g., full-time, part-time, permanent, temporary)
- Salary and remuneration details
- Performance reviews and appraisal records
- Training and professional development records

3. Recruitment Information:
- Application forms and supporting statements
- Curriculum Vitae (CV)
- References from previous employers
- Right to work documentation and immigration status
- Criminal records checks, where applicable

4. Financial Information:
- Bank account details for salary payments
- Tax and National Insurance contributions
- Pension scheme details
- Benefits and allowances

5. Health and Wellbeing Data:
- Sickness and absence records
- Medical or health information, including occupational health assessments
- Disability information and any required workplace adjustments

6. Equal Opportunities Monitoring:
- Ethnicity
- Religious beliefs
- Sexual orientation
- Gender identity
- Information on disabilities

7. Emergency Contact Details:

- Names and contact information of next of kin or designated emergency contacts

8. IT, Estates and Communications Usage:
- Access logs for university facilities and systems
- Records of communications sent via university platforms
- CCTV images, in accordance with our CCTV Policy.

9. Legal and Compliance Records:
- Records of grievances, disciplinary actions, and investigations
- Compliance training records (e.g., data protection, health and safety)

10. Additional Information:
- Declarations of personal relationships, in line with the Personal Relationships Policy.

It's important to note that some of this data, such as information on ethnicity, health, and criminal convictions, is classified as "special category" data under data protection laws and is subject to stricter processing conditions. Where the organisation processes special categories of personal data, for example information relating to your ethnicity, sexual orientation, health or religion or belief; access to, and the sharing of, this information is controlled very carefully. You will be given more details about our use of any special category personal data when we collect it from you. You can review and update your personal data at any time through the University's self-service system MyView, to ensure that we hold accurate and up to date information about you.

Why Are We Processing Your Personal Data

The organisation collects and processes personal data relating to its employees, workers, volunteers, consultants, and contractors to manage the employment relationship. The organisation is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations in accordance with GDPR. This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time.

The organisation needs to process data to enter into an employment contract with you and to meet its obligations under your employment contract. For example, it needs to process your data to provide you with an employment contract, to pay you in accordance with your employment contract, and to administer pension entitlements.

In some cases, the organisation needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check an employee's identity and entitlement to work in the UK, to deduct tax, to comply with health and safety laws, and to enable employees to take periods of leave to which they are entitled.

Processing employee data allows the organisation to:

- Run recruitment and promotion processes.
- Maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights.
- Operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace.
- Operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and workforce management purposes.

- Operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled.
- Obtain occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled.
- Operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that the organisation complies with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled.
- Ensure effective general human resourcing and business administration.
- Provide references on request for current or former employees.
- Respond to and defend against legal claims.
- Ensure employees can operate self-service portals such as MyView and the Self-Service Password Reset Service (SSPRS).

How Your Data Is Collected

Data is collected when you provide it to the University prior to, at commencement of, and during employment. This may be through correspondence with you, interviews, declarations, meetings, or other assessments.

Prior to employment, this is through your application form and supporting documents such as a Curriculum Vitae (CV) or cover letter.

For some parts of our application process, we use third-party processors to check your Right to Work, authenticate your personal identity documents, and manage our recruitment process.

At commencement of employment, you provide additional data to allow us to legally employ you, pay you, and communicate with you effectively.

Throughout your employment, you may be asked to provide further data in relevance to a function or specific task or to check or update information such as contact details.

In some cases, the organisation collects personal data about you from third parties, such as references supplied by former employers, recruitment agencies, information from employment background check providers, professional bodies, information from credit reference agencies (where applicable), and information from criminal records checks permitted by law.

How Your Data Is Stored Internally and Accessed

Data is stored in a range of different places including:

- In your personnel file – electronic and hard copy.
- In the organisation's human resource management systems (including the POD and Payroll system, Self-Service Portal MyView, Performance Management and Appraisal system, timetabling, and workload allocation system).
- In Microsoft 365 applications such as emails, documents, spreadsheets, and collaboration tools (e.g. Teams chats and SharePoint sites).

- In other IT systems used by the University of Suffolk.
- University provided devices and any and all data held on University devices, including emails, SharePoint, OneDrive and any other University systems, can be accessed if there is a business-critical need in the event of an employee's absence. For this reason, staff should not use University devices for personal business. In the event access is needed, this will be requested from the line manager and approved by Data Governance on a case-by-case basis.

Use of Artificial Intelligence (AI) in Minerva

The University of Suffolk uses artificial intelligence (AI) within its Minerva service platform to support staff and student queries.

What this means

- You may interact with an AI-powered assistant when using Minerva
- The AI will only use University-approved knowledge base information

Your data

- Your personal data does not leave the University's Minerva system
- Data is not shared with external AI providers
- Data is not used to train external AI models
- Confidential or sensitive enquiries are excluded from AI processing

Transparency

- You will always be informed when you are interacting with AI
- You may choose alternative support routes if you prefer

Safeguards

- The AI does not make decisions affecting you
- Staff review and validate outputs before action is taken
- If the AI cannot assist, or if your query relates to wellbeing or urgent support, it will direct you to appropriate human support services already identified on the safeguarding pages.

Your rights

- You retain all rights under UK GDPR, including access to your data and how it is used
- For queries relating to data use, please contact Data Governance

How Your Data is Shared

Your information will be shared internally, including with members of the POD (People and Organisational Development) team, your line manager, managers in the business area in which you work, Planning and Management Information and Digital and IT staff if access to the data is necessary for performance of their roles.

The organisation shares your data with third parties for payroll purposes, external training platforms, customer relationship management systems, to obtain pre-employment references from other employers, obtain employment background checks from third-party providers, and obtain necessary criminal records checks from the Disclosure and Barring Service. In those circumstances, the data will be subject to confidentiality arrangements.

The University will make some statutory and routine disclosures of personal data to third parties where appropriate. These third parties include:

- Higher Education Statistics Agency (HESA).
- Universities and Colleges Employers Association (UCEA).
- UK Visas and Immigration (UKVI).
- HM Revenue and Customs (HMRC).
- Pension schemes – including the Local Government Pension Scheme (LGPS) and the Universities Superannuation Scheme (USS) (as set out in the scheme rules).
- Research sponsors/funders.
- Trade unions.
- Potential employers (where a reference is requested).
- 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).
- Payroll Service.
- Occupational Health provider.
- Employee Assistant Programme.

Personal data may also be disclosed when legally required (for example under UK GDPR or the Freedom of Information Act) or where there is a legitimate or vital interest, either for the University, the data subject or requesting party, considering any prejudice or harm that may be caused to the data subject.

As a benefit of employment at the University of Suffolk, you have access to sign up to additional services e.g. counselling etc. These services are consent-based, and the employee should take note of the Privacy Notice provided by the third party. The University of Suffolk does not share personal data with the third party other than to confirm your employment and therefore eligibility for the service.

The University may also use third-party companies as data processors to carry out certain administrative functions on behalf of the University. If so, a written contract will be put in place with that processor to ensure that any personal data disclosed will be held in accordance with the Data Protection Legislation.

We may transfer your personal data outside the UK, for example, when we use third-party providers to help deliver our services, such as cloud or externally hosted software providers. These providers may store or process personal data in countries outside the UK. Whenever we transfer your personal information to a third party or to another country, we ensure it is

protected in line with data protection laws. This includes putting in place appropriate safeguards, such as contracts that contain the UK's approved standard data protection clauses, where the destination country does not have an adequate level of data protection.

How Long Is the Data Kept For

Personal data is held for the duration of employment. The periods for which your data is held after the end of employment are set out in the relevant data retention schedule and may depend on the position held.

Changes to This Privacy Notice

We may update this privacy notice at any time. We may also notify you in other ways from time to time about the processing of your personal information.

Data Subject Rights

One of the aims of GDPR is to empower individuals and give them control over their personal data. The GDPR gives you the following rights:

- The right to be informed.
- The right of access.
- The right to rectification.
- The right to erasure (or the right to be forgotten)
- The right to restrict processing.
- The right to data portability.
- The right to object.
- Rights in relation to automated decision-making and profiling.

Contact Information

If you have any questions about this privacy notice or about exercising any of your rights under GDPR, please contact the Data Governance team on datagovernance@uos.ac.uk.