University of Suffolk

University of Suffolk

Privacy Information Notice for Employees and other Workers

Data controller: University of Suffolk

Data protection officer: Fiona Fisk, dataprotection@uos.ac.uk

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 the General Data Protection Regulation (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.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

What information does the organisation collect?

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

- All personal details supplied by you on your application form, CV etc. including your name, address and contact details, including email address and telephone number, date of birth gender;
- Copies of ID – such as passport, birth certificate, utility bill as provided;
- the terms and conditions of your employment;
- details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the organisation;
- information about your remuneration, including entitlement to benefits such as pensions , insurance cover or statutory and occupational sick pay;
- details of your bank account and national insurance number;
- copies of any correspondence from a government agency as applicable, e.g. child support agency;
- information about your marital status, next of kin, dependants and emergency contacts;

- information about your nationality and entitlement to work in the UK;
- information about your criminal record;
- details of your schedule (days of work and working hours) and attendance at work;
- details of periods of leave taken by you, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave;
- details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence;
- assessments of your performance, including appraisals, performance reviews and ratings, training you have participated in, performance improvement plans and related correspondence;
- information about medical or health conditions, including whether or not you have a disability for which the organisation needs to make reasonable adjustments;
- details of trade union membership; and
- equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief voluntarily supplied by you.

The organisation collects this information in a variety of ways. For example, data is collected through application forms, CVs or resumes; 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 (such as benefit nomination forms); from correspondence with you; or through interviews, meetings or other assessments.

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

Data is stored in a range of different places including:

- in your personnel file;
- in the organisation's HR management systems (including the HR & Payroll system, Performance Management & Appraisal system, timetabling and workload allocation system); and
- in other IT systems (including the organisation's email system).

Why does the organisation process personal data?

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. For certain positions, it is necessary to carry out criminal records checks to ensure that individuals are permitted to undertake the role in question. Under the Equality Act 2010, the organisation also has a duty to maintain and promote equality.

In other cases, the organisation has a legitimate interest in processing personal data before, during and after the end of the employment relationship.

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 HR and business administration;
- provide references on request for current or former employees;
- respond to and defend against legal claims;

Some special categories of personal data, such as information about health or medical conditions, is processed to carry out employment law obligations (such as those in relation to employees with disabilities and for health and safety purposes). Information about trade union membership is processed to allow the organisation to operate check-off for union subscriptions.

Where the organisation processes other special categories of personal data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is done for the purposes of equal opportunities monitoring. Data that the organisation

uses for these purposes is anonymised or is collected voluntarily from employees, workers, volunteers, consultants or contractors. We only process this information with your explicit consent, which can be withdrawn at any time by completing the appropriate fields on MyView, the University of Suffolk's self-service system. You are entirely free to decide whether or not to provide such data and there are no consequences of failing to do so.

Who has access to data?

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

The organisation shares your data with third parties in order 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 (University of East Anglia)
- Occupational Health provider

Personal data may also be disclosed when legally required or where there is a legitimate interest, either for the University or the data subject, taking into account any prejudice or harm that may be caused to the data subject.

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.

The organisation will not transfer your data to countries outside the European Economic Area, should there be any changes to this in the future, we you will be notified of the changes and the relevant safeguards put in place.

How does the organisation protect data?

The organisation takes the security of your data seriously. The organisation has internal policies and controls in place to try 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. Further details of these can be found on the University's intranet. Where the organisation engages third parties to process personal data on its behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

For how long does the organisation keep data?

The organisation will hold your personal data for the duration of your employment. The periods for which your data is held after the end of employment are set out in the relevant data retention schedule.

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 organisation to change incorrect or incomplete data;
- require the organisation to delete or 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 organisation is relying on its legitimate interests as the legal ground for processing; and
- ask the organisation to stop processing data for a period if data is inaccurate or there is a dispute about whether or not your interests override the organisation's legitimate grounds for processing data.

If you would like to exercise any of these rights, please contact

Data Protection Officer, Fiona Fisk, *dataprotection@uos.ac.uk*

You can make a subject access request by completing the University's form for making a subject access request.

If you believe that the organisation has not complied with your data protection rights, you can complain to the Information Commissioner.

What if you do not provide personal data?

You have some obligations under your employment contract to provide the organisation with data. In particular, 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 also have to provide the organisation with data in order to exercise your statutory rights, such as in relation to statutory leave

entitlements. Failing to provide the data may mean that you are unable to exercise your statutory rights.

Certain information, such as contact details, your right to work in the UK and payment details, have to be provided to enable the organisation to enter a contract of employment with you. If you do not provide this information, this will hinder the organisation's ability to administer the rights and obligations arising as a result of the employment relationship efficiently.

Automated decision-making

Employment decisions are not based solely on automated decision-making.

Changes to this privacy notice

We may update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

Privacy notices may be viewed at any time on the University's website.

If you have any questions about this privacy notice, please contact Data Protection Officer, Fiona Fisk, *dataprotection@uos.ac.uk*

I,_____ (name), acknowledge that on _____ (date),

I received a copy of the University of Suffolk's Privacy Notice for Employees and other Workers and that I have read and understood it.

Signature

……

Name

……