

PRIVACY NOTICE EMPLOYEES, WORKERS AND CONTRACTORS

The University of Chichester (the **University**) is committed to protecting the privacy and security of your personal information. This privacy notice describes how we, as a data controller, collect and use personal information about you prior to, during and after your working relationship with us, in accordance with applicable data protection legislation. This notice applies to applicants, current and former employees, workers and certain contractors. 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.

This notice should be read alongside the University of Chichester Privacy Standard, available from the Data Protection Officer, or online here:

<https://www.chi.ac.uk/about-us/policies-and-statements/data-protection>

1. Legal bases and purposes for processing personal data

The University collects and uses data about you in order to fulfil contractual, statutory and management responsibilities during the recruitment phase and throughout your employment and after your employment with the University.

1.1. Legal bases

Personal data is processed in accordance with the data protection legislation and is normally provided to the University by applicants and members of staff on an application form, contracts of employment and associated documentation. In addition to the information provided by yourself, the University may hold information about you provided by other sources. This includes the taking up of references on appointment, occupational health reports and performance information received by your manager, such as annual appraisals. On employment, the University will generate a unique employee number, which will be used as a personal reference. The personal data provided by yourself and others is primarily processed in order to fulfil contractual obligations. The University also processes your personal data to comply with any legal and statutory obligations, to protect the vital interests and to pursue the legitimate interests of the University.

1.2. Examples of personal data processed

We will process the following categories of personal information about you:

- Personal details, such as name, title, address, contact details.
- Date of birth.

- Gender.
- Marital status.
- Next of kin and emergency contact information.
- National insurance details.
- Start date.
- Bank account details and tax status information.
- Salary, pensions and benefits information.
- Recruitment information, such as previous employment details, highest qualifications, right to work documentation, references, and interview notes.
- Disclosure and Barring Service record number and issue date (where relevant to the role).
- Performance information (including probationary reviews, appraisals and capability records).
- Disciplinary and grievance information.
- CCTV footage.
- Photograph for the purposes of staff identification and access to University buildings/facilities via a staff campus card.
- Information about your use of University computers and electronic equipment.
- Copies of correspondence (e.g. emails and letters) relating to your employment at the University.

We may also process the following “special categories” of data:

- Data for statutory returns and for the purposes of monitoring equal opportunities, including race, religious beliefs, disability and sexual orientation.
- Trade union membership for the purpose of payroll deductions.
- Information about your health, including a pre-employment health assessment, sickness records, medical conditions and occupational health referrals for the purposes of ensuring capability to undertake your role, managing sickness absence and ensuring the health, safety and wellbeing of you or others.

“Special categories” of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the following circumstances:

- In limited circumstances, with your explicit written consent.
- Where we need to carry out our legal and statutory obligations and in line with the University of Chichester Privacy Standard.
- Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our occupational pension scheme, and in line with the University of Chichester Privacy Standard.

- Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.
- Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public. We may also process such information about existing and former employees in the course of legitimate business activities with the appropriate safeguards.

1.3. Purposes of processing personal data

The purposes of processing personal data can broadly be categorised under the following headings:

- **Contract and employment related administration**
This will include recruitment/appointment to a role, determining terms and conditions, administering changes to your contract, making decisions related to your role (e.g. promotion, fractionalisation, flexible working requests), performance information (e.g. probationary reviews and appraisals), training and development, disciplinary, grievance and capability matters (including ill health) and matters relating to the end of your contract (e.g. resignation, redundancy, retirement). Contract administration also covers paying you, making necessary deductions (e.g. tax, NI, pension contributions, salary sacrifice schemes, trade union membership) and liaising with pension providers.
- **Legal and statutory obligations**
This will include statutory returns to the Higher Education Statistics Agency (HESA), information required by the Higher Education Funding Council for England (HEFCE) and partner bodies. In addition, the University may have a legal obligation to process certain personal information (e.g. evidence of right to work in the UK) and may hold personal data for the purposes of preventing fraud and dealing with legal disputes.
- **Use of University facilities, buildings and equipment**
This will include a photographic staff card for accessing buildings and using facilities (e.g. library), security and ensuring compliance with the University's Electronic Information Security Policy and IT Code of Conduct.
- **Equal opportunities monitoring and reporting purposes**
The University records personal information for equal opportunities monitoring and compliance with obligations such as gender pay gap reporting. Your personal information may also be analysed in order to report on HR related issues (e.g. sickness absence, turnover, recruitment, professional development).
- **To protect your vital interests or the vital interests of others.**
This will include health and safety obligations e.g. accidents at work and contacting you or a next of kin in an emergency situation, or where there is concern for your welfare.

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our employees).

1.4. Information about criminal convictions

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us. University staff may be required to hold a Disclosure Certificate from the Disclosure and Barring Service. The Certificate is proof that the individual concerned does not have any previous conviction under the Rehabilitation of Offenders Act 1974, which could be relevant to their work at the University. Further information is available in interview documentation.

1.5. Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

2. The recipients of personal data

Whilst data collected and maintained by Human Resources Department will in normal circumstances not be disclosed without your consent, the University will disclose that data to authorised personnel within and outside of the University in certain circumstances, examples of which are below:

2.1. iTrent

Your personal details and information related to your employment and pay are stored on iTrent. iTrent is a HR and Payroll system provided by MHR International UK Limited (MHR) and data is stored in compliance with data protection legislation. MHR are required to take appropriate security measures to protect your personal information in line with our policies.

2.2. HESA

As a Higher Education Institution we are legally obliged to supply the Higher Education Statistics Agency (HESA) with data relating to staff, students, Facilities' and Finance on an annual basis. We submit this data to HESA via a secure link in September of each year. For further detail about the collection of data and its subsequent use please see the [HESA Fair Collection Notice for Staff](#) for further details.

2.3. HEFCE

The University may need to disclose personal data to HEFCE and its partner bodies. This may include providing data in support of its application during a Research Excellence Framework (REF) or Teaching Excellence Framework (TEF) assessment.

2.4. Government Departments

Under certain circumstances the University may be asked by Government departments (e.g. UK Visas & Immigration, Police, HMRC) to disclose personal information for matters relating to the prevention and detection of crime, apprehension and prosecution of offenders or the collection of tax.

2.5. Freedom of Information and Environmental Information Regulations requests

The University is subject to the Freedom of Information Act and Environmental Information Regulations. The University may at times be required to disclose personal information, where the disclosure does not breach data protection legislation.

2.6. Occupational Health Provider

Pre-employment health assessments and occupational health referrals are carried out by Working Health Solution. During the course of your employment, it may be necessary to refer you to an occupational health physician to provide independent advice and support related to sickness absence, to ascertain your capability to undertake your role, to advise on medical conditions and where a role-specific risk assessment has been undertaken (e.g. night work, use of powered machinery).

2.7. Writing references for a third party (e.g. employment, mortgage, rental, education)

On occasion, we will be asked to provide references for external agencies and organisations. This may include confirmation of employment dates, salary and opinions on performance. Before providing personal information, confirmation will be sought from the data subject that the information can be provided, or the third party will be asked to provide evidence that consent has been given.

2.8 Pension providers

The University is required to provide relevant information to pension providers, including Local Government Pension Scheme (LGPS), Teachers' Pensions (TP) and Universities Superannuation Scheme (USS) for the successful administration of employee pensions.

The University may on occasion make other disclosures without your consent. This will always be done in accordance with the relevant data protection legislation.

3. Photography and filming

We store the photograph used on your staff Campus Card. We will not display your photograph internally (e.g. staff intranet pages) without advising you that we have done so and giving you the right to object. We will not display your photograph externally (e.g. external website) or release your photograph outside the University without consent. Your photo will be deleted at the point your employment with University ceases.

The University may also occasionally commission photographs around the campuses or at specific events such as Graduation for inclusion in promotional material. If you do not want to appear in publicity materials please make yourself known to the photographer.

You should be made aware e.g. via location warning notice, verbally or via a consent process prior to the taking of photographs or film recording, both of the purposes and the location(s) where the photographs or film will be made available e.g. University web pages/intranet.

Some areas of the University are accessible to the public, e.g. the LRCs so they will be considered public areas. This means that filming or photography may take place, which incidentally capture passers-by in the background, without the need to get their consent. A Location Warning Notice for Filming/Photography should be displayed, so that you are aware that this might happen.

4. Third country transfers

The University does not transfer your personal details to a third country unless for specific purposes and where you have knowingly provided personal information explicitly for that purpose. Examples include when bidding for international research funds or for the purposes of exchange programmes (e.g. Erasmus).

5. Retention of your personal data

The University will only keep your data for as long as necessary. Most of your personal information will be retained for a period of six years after you have ceased employment. This is in line with best practice and guidance, based on the need to retain information in case of a legal claim against yourself or the University. After this period, some information will be retained in order to deal with pension-related queries and in order to confirm periods of employment, salary and job roles in references to future employers. A full retention schedule is available from the Data Protection Officer (see para 8 below for contact details).

6. Automated decision-making

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:

- Where we have notified you of the decision and given you 21 days to request a reconsideration.
- Where it is necessary to perform the contract with you and appropriate measures are in place to safeguard your rights.
- In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

If we make an automated decision on the basis of any particularly sensitive personal information, we must have either your explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights.

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

7. Data Subject rights

7.1. Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us. Certain personal data (e.g. name, address, bank details, special categories of data) can be updated by individuals through their HR Self Service Portal. Staff are encouraged to periodically check their personal information to ensure it is up-to-date and accurate. Where personal information changes, you can also email HR@chi.ac.uk in order to update your records.

7.2. Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

- **Request access to your personal information** (commonly known as a “data subject access request”). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- **Request correction of the personal information** that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure of your personal information.** This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- **Request the restriction** of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact DPOfficer@chi.ac.uk.

7.3. Fees

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly

unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

7.4. What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

7.5. Right to withdraw consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact HR@chi.ac.uk. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

8. Contact details and further information

The University of Chichester's Data Protection Officer (Su Longden) can be contacted via email at DPOfficer@chi.ac.uk. Alternatively, written requests and queries can be sent via post to the Data Protection Officer, University of Chichester, College Lane, Chichester, West Sussex. PO19 6PE. If you have any queries about how your personal data is processed you can contact HR@chi.ac.uk.

You have a right to lodge a complaint at any time with the Information Commissioner's Office (ICO), the supervisory authority for data protection issues.

For further information on data protection at the University, please see the University of Chichester Privacy Standard:

<https://www.chi.ac.uk/about-us/policies-and-statements/data-protection>

Version control:

1.0	6 March 2018	
1.1	23 May 2018	Clause 2.8 added; typos corrected.