Recruitment Privacy Notice

# Introduction

The University of Southampton is a "Data Controller". This means that we are responsible for deciding how we hold and use personal data about you. We are required under data protection legislation to notify you of the information contained in this Recruitment Privacy Notice.

This Notice sets out how we comply with our data protection obligations and seek to protect personal information relating to our job applicants. Its purpose is to make you aware of how and why we are using your personal data and what your rights are under data protection legislation. It is important that you read and retain this document.

This Notice does not form part of your terms and conditions of employment or other contract to provide services, nor is any part of it intended to have contractual effect. We may amend this Notice at any time but if we do so a current version can be obtained [here](https://www.southampton.ac.uk/hr/services/data-protection/data-protection.page); however, it remains your responsibility to be familiar with and comply with the terms of the Recruitment Privacy Notice which are in force at any time.

Please be aware that we may provide you with other privacy notices on specific occasions when we are collecting or processing personal data about you (such as a website privacy notice). This Recruitment Privacy Notice is not intended to exclude or supersede provisions in any such other privacy notices that may apply to you.

We collect and process personal data relating to our job applicants to help us manage the recruitment process. We are committed to being transparent about how we collect and use that data and to meet our data protection obligations.

We recognise the need to treat the personal data we hold about you (“your Data”) in an appropriate manner and process it in accordance with the General Data Protection Regulation (GDPR) (EU) 2016/679 as it forms part of domestic law in the United Kingdom by virtue of section 3 of the European Union (Withdrawal) Act 2018 and [DPPEC (Data Protection, Privacy and Electronic Communications (Amendment Etc.) (EU Exit)) Regulations 2019](https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.legislation.gov.uk%2Fuksi%2F2019%2F419%2Fcontents%2Fmade&data=04%7C01%7CC.J.Trotter%40soton.ac.uk%7C24ba064afdf04e74e73208d8d8a218de%7C4a5378f929f44d3ebe89669d03ada9d8%7C0%7C0%7C637497537992438487%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=3aVLzIdeRyYdOJO8LwIBVtC5K6aTkP07piqSyUUG8Uo%3D&reserved=0) (including as further amended or modified by the laws of the United Kingdom or of a part of the United Kingdom from time to time) (UK GDPR), the UK Data Protection Act (DPA) 2018, and the University Data Protection Policy (a current version of which can be obtained [here](http://www.southampton.ac.uk/assets/sharepoint/intranet/ls/Public/Information%20Governance%20Policies/Data%20Protection%20Policy.pdf)).

Data refers to the information that we hold about you from which either on its own or in combination with other information you can be identified and may include names, contact details, photographs, identification numbers, online identifiers, and expressions of opinion about you, or person-specific indications as to our intentions about you. A non-exhaustive list of the types of Data we collect about our employees is set out below.

"Processing" means doing anything with your Data, such as collecting, recording or holding the Data as well as disclosing, destroying or using the Data in any way.

# 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.

# Why does the University process personal data?

We process your Data with your consent to enable us to process your job application made to the University and to complete the recruitment process.

In some cases, we need to process your personal data to ensure that we are complying with our legal obligations. For example, we are required to check a successful applicant's eligibility to work in the UK before employment starts.

The University also has a legitimate interest in processing your Data during the recruitment process and for keeping records of the process. Processing data from job applicants allows us to manage the recruitment process, assess and confirm a candidate's suitability for employment and decide the successful candidate. We may also need to process data from job applicants to respond to and defend against any legal claims.

We will use the Data we collect about you to:

* Assess your skills, qualifications, and suitability for the role
* Carry out background and reference checks, where applicable
* Communicate with you about the recruitment process
* Keep records related to our hiring processes
* Comply with legal or regulatory requirements.

It is in our legitimate interests to use the data you have provided to help us decide whether it is appropriate and beneficial to the University to appoint you to the role and whether to enter into a contract of employment with you.

Having received your application form and supporting material and any additional information obtained via our recruitment and selection processes, we will process that information to decide whether you meet the basic requirements to be shortlisted for the role. If you do, we will decide whether your application is strong enough to invite you for an interview. If we decide to call you for an interview, we will use the information you provide to us at the interview to decide whether to offer you the role. If we decide to offer you the role, we will then take up references, confirm your right to work in the UK, carry out a criminal record check (if relevant to the role you have applied for) and carry out other checks (if relevant to the role) before confirming your appointment.

We may also need to process your Data to comply with our legal obligations and, if it is necessary, to process it for the protection of your vital interests, for our legitimate interests or the legitimate interests of others.

Where we rely on our, or another’s, legitimate interests as a reason for processing your Data, we have considered whether or not those interests are overridden by your rights and freedoms and have concluded that they are not.

# Processing for limited purposes

We will only process your data for the specific purpose or purposes that we tell you about or if specifically permitted under any privacy legislation and will only process your data to the extent necessary for that specific purpose or purposes.

# What information does the University collect?

We collect and process a range of information about you in order to manage your application to us. This includes the following types of Data:

* Biographical information about you, including your name, address and contact details, including email address and telephone number, date of birth and gender
* Details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the University
* Details of your bank account where you have chosen payment to be made
* Your national insurance number
* Information about your nationality and entitlement to work in the UK
* Information about your criminal record, if relevant to the job you are applying for
* Information about medical or health conditions, including whether or not you have a disability for which the organisation needs to make reasonable adjustments
* Information about your availability to allow us to organise our timetabling system (if applicable to your role)
* Equal opportunities monitoring information including information about your ethnic origin, sexual orientation and religion or belief.

# Information about criminal convictions

If applicable to your role, we are entitled to carry out a criminal records check in order to satisfy ourselves that there is nothing in your criminal convictions history which makes you unsuitable for the role you have applied for. This may involve us sharing certain parts of your Data with a third party organisation that provides the checking service.

We will only share your Data for this purpose, and collect information about your criminal convictions history in response, if you have given us your consent to do so, or we are required to do so by law. We will only collect this information if we would like to offer you a role where your criminal convictions history is relevant to the role and subject to other checks and conditions, such as references, being satisfactory.

# How the University uses your Special Category Data

Special category data is personal data that the data protection legislation says is more sensitive, and so needs more protection. It includes information about an individual’s race, ethnic origins, politics, religion, trade union membership, genetics, biometrics (where used for unique identification purposes), health, sex life, or sexual orientation.

Some special categories of personal data, such as information about health or medical conditions, are processed to carry out employment law obligations (such as those in relation to employees with disabilities).

Where we process other special categories of your Data, such as information about ethnic origin, sexual orientation, or religion or other beliefs, this is done for limited necessary purposes, including equal opportunities monitoring and to meet the requirements of Higher Education Statistics Agency (HESA) reporting.

We do not need your consent if we use special categories of your Data to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the data that we would like to process and the reason, so that you can carefully consider whether you wish to consent. You are under no obligation to provide data for equal opportunities monitoring purposes and there are no consequences for your application if you choose not to provide such data. We may collect and process special categories of your Data in the following circumstances:

* In limited circumstances where absolutely necessary on the basis of your written consent obtained in advance of the processing activity
* Where it is needed to serve the public interest, such as for equal opportunities monitoring of our recruitment processes
* Where it is needed in relation to bringing and defending legal claims, or where it is needed to protect your (or someone else's) vital interests and you are not capable of giving your consent
* Where you have already manifestly made special categories of personal data public.

We will collect and use the following particular types of your Data of a specific special category nature in the following ways:

* We will use information about your physical or mental health, or disability status, to ensure your health and safety and provide appropriate adjustments should you be invited to interview,
* With your consent, we will collect and use data about your race, national or ethnic origin, religious, philosophical, or moral beliefs, and/or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting, for example, to meet the requirements of equal opportunity reporting. Such data will be aggregated with other job applicants’ data so that you are not personally identifiable to any third-party organisation with which we are required to share this information. You can withdraw your consent at any time, and there are no consequences if you choose not to provide such data.

# What if you decide not to provide us directly with your personal data for processing in the employment relationship?

You are under no statutory or contractual obligation to provide your data to us during the recruitment process. However, if you do choose not to provide the information, we may not be able to process your application properly or at all.

You are under no obligation to provide information for equal opportunities monitoring purposes and there are no consequences for your application if you choose not to provide such information.

# How will your personal data be collected?

We may collect your Data in a variety of ways. For example, personal information might be collected directly from you (through application forms, CVs or resumes); obtained from your passport or other identity documents such as your driving licence (for identity authentication purposes); from correspondence with you; or through interviews, or other meetings and assessments that form part of the recruitment activity.

We may also collect personal data about you from third parties, such as references supplied by former employers (nominated by you), UK Visa and Immigration, information from employment background check providers and information from criminal records checks.

We will usually only seek information from third parties once a job offer to you has been made and will inform you that we are doing so. If you are applying for an academic role, we may seek references from your referees before a job offer is made to you.

We will always look to ensure that any third party has the lawful authority to share this Data with us.

We may review publicly available information about you, including your social media presence, if such a review is relevant to the role you are applying for and it is in our legitimate interests to do so. We also recognise your right to privacy over that information and your right to object to our processing that publicly available information for our own purposes.

# Where will your personal data be stored?

Your personal data will be stored in a range of different places, including in the eRecruit system, the University’s HR management systems and in other IT systems (including the University's email system).

# Holding and retaining your data

We collect, create, and store your Data both electronically and on paper throughout the recruitment process. We will only hold your Data as long as is necessary for the purpose or purposes that we have collected it.

Unsuccessful applications will be held within the eRecruit system for a period of up to one year before being deleted in order that you can access and re-use data in future applications and we can respond to statutory reporting requests.

Successful applicant data will be transferred to our HR systems.

You can obtain full details of our retention schedule [here](https://www.southampton.ac.uk/hr/services/data-protection/data-protection.page).

# Who has access to your personal data?

Your Data will be shared internally within the University, as necessary, for the purposes of the recruitment exercise:

* Interviewers/line management (and their nominated delegates) involved in the recruitment process
* Other internal teams as may occasionally require access to your Data for the fulfilment of their roles related to the proper functioning of the University.

We also share certain information about you with third parties external to the University. This may include, for example, the following types of disclosures of your Data as relevant to a job applicant:

* Any referees nominated by you
* Any third parties involved in a shared recruitment activity
* UK Visa and Immigration where a visa is required to work and, with your permission, Digital Identity Service Provider for right to work checks.
* Disclosure Barring Service where a criminal records check is required for the employment role you perform and, with your permission, a third-party supplier to perform a check online.

We will not share your data with third parties, unless your application for employment is successful and we make you an offer of employment. We will then share your data with former employers to obtain references for you, employment background check providers to obtain necessary background checks (if relevant to the role), UK Visa and Immigration and the Disclosure and Barring Service to obtain necessary criminal records checks (if relevant to the role). Please note that references for academic posts may be sought prior to a job offer.

Some information about you may be transferred outside the European Economic Area (EEA) should you apply for a role that is based in another country. For example, some of your Data may be transferred outside the EEA on the basis of your application for a job at one or more of the University’s international establishments, and/or our compliance with our legal obligations (both UK and locally to the establishment you have applied to work at), as well as our obligations under the contract of employment we enter into with you (such as occupational entitlements).

We may have to disclose your Data if required to do so by law in order to comply with a legal obligation, to protect our rights, interests or property and those of others, act in urgent circumstances to protect the personal safety of our staff, students, and the public, or to protect us against any legal liability.

# How do we protect your personal data?

We have put in place appropriate security measures to prevent your Data from being accidentally lost, used or accessed in an unauthorised way, altered, or disclosed. In addition, we limit access to your Data to those employees, agents, contractors and relevant other third parties who have a business need-to-know. They will only process your Data on our instructions and they are subject to a duty of confidentiality.

Our staff have a legal duty to keep your Data confidential. There are strict codes of conduct in place to keep your Data safe. Staff must abide by the GDPR, the DPA, and the University Data Protection Policy.

We endeavour to ensure that suitable organisational and technical measures are in place to prevent the unlawful or unauthorised processing of your Data, and to ensure against the accidental loss of or damage to your Data. This includes:

* Storing Data on an appropriately secure system
* Training all our staff in their data protection responsibilities
* Working with reputable companies for data processing services, in particular those that are data protection compliant and willing to enter into appropriate data sharing agreements with us
* Ensuring that appropriate protection and agreements are in place when we work with trusted organisations based outside the European Economic Area (EEA).

Where we engage third parties to process personal data on our 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.

# Automated decision making and profiling

None of the Data collected about you as part of this recruitment exercise will be used as part of any automated decision making or to build a profile of you as part of the recruitment exercise.

If you have any concerns or queries about the decision making process, please contact us by email at: AskHR@soton.ac.uk

# Your rights

You have a number of rights. You can:

* Access and obtain a copy of your Data on request
* Require us to change incorrect or incomplete Data
* Require us 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 we are relying on our legitimate interests as the legal ground for processing; and
* Ask us to stop processing your Data for a period of time if you are concerned that any data we hold about you is inaccurate, or if 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 us at: AskHR@soton.ac.uk

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

# Right to withdraw consent

Consent may be withdrawn at any time where it is the sole basis for processing. When you applied for this role, you provided consent to us processing your personal information for the purposes of the recruitment exercise.

To withdraw your consent, please contact AskHR@soton.ac.uk. Once we have received notification that you have withdrawn your consent, we will no longer process your application and, subject to our retention schedule, we will dispose of your personal data securely.

# How do you access your data?

You can view and change some of the personal data held by us through self-service on the eRecruit system.

Alternatively, if you are unable to self-serve, you can also contact us if your details change or if you feel that the Data we hold about you for recruitment purposes is inaccurate or incomplete email AskHR@soton.ac.uk

In certain circumstances you can request your data for reuse for your own purposes across different services. If you require any further assistance with this please email AskHR@soton.ac.uk.

If you would like to submit a subject access request for Data stored on your recruitment record held by the HR eRecruit system, please make a request in writing via: <https://www.southampton.ac.uk/about/governance/subject-access-request-form.page>

Or by writing to The Data Protection Officer, Legal Services, University of Southampton, Highfield, Southampton SO17 1BJ.

# Accurate personal data

We will keep your Data accurate and up to date. Personal information that is inaccurate or out of date will be destroyed where its retention is no longer needed by us for a legitimate purpose (such as Payroll records).

Once you have submitted your application via eRecruit you will not be able to change any of the application details, including your personal data, in respect of this job application.

You do have control over your recruitment related data through your logon to the eRecruit system and can change, update and delete as you wish for **future** job applications.

If you are unable to access eRecruit to manage your Data, please let us know if your details change, or, if you feel that the Data we hold about you is inaccurate, please email AskHR@soton.ac.uk.

# Further information

We also have additional policies and guidelines concerning particular activities. If you would like further information please see our Publication Scheme at: <http://www.southampton.ac.uk/about/governance/regulations-policies-guidelines.page#publication_scheme>.

If you are unhappy with the way that we have handled your data you can contact us using this [online form](https://sotonproduction.service-now.com/com.glideapp.servicecatalog_cat_item_view.do?sysparm_id=c8b9f388db769b006f3df57eaf96193d) or contact the Information Commissioner’s Office. See their website at: <https://ico.org.uk/>. We would, however, appreciate the chance to deal with your concerns before you approach the ICO so please do contact us in the first instance.

The University of Southampton is the Data Controller and our registration number with the Information Commissioner’s Office is Z6801020.

# Recruitment Privacy Notice

## Please sign and return

Please complete and return this slip to:

Recruitment

University of Southampton

Building 26, Highfield
Southampton

SO17 1BJ

I acknowledge that I have received a copy of the University of Southampton’s Applicant Privacy Notice and that I have read and understood it.

|  |  |
| --- | --- |
| Signed |  |
| Name |  |
| Date |  |
| Job reference number (if known) |  |

VERSION CONTROL

|  |  |
| --- | --- |
| Version | 3.2 |
| Last updated:  | 1 October 2022 |
| Consulted: | HRSLT |
| Feedback: | Updated to reflect use of third party right to work check provider |
| Author: | Christine Trotter – Head of HR Operations |