



St Mary's University Twickenham London

Human Resources

PRIVACY NOTICE FOR JOB APPLICANTS AND CANDIDATES

1. WHAT IS THE PURPOSE OF THIS DOCUMENT?

St Mary's University (also referred to as "the University", "we", "our" and "us") is committed to protecting the privacy and security of your information.

This privacy notice describes how we collect and use your personal information when you apply for a job with the University.

Personal data" is any information that relates to an identifiable natural person. Your name, address, contact details and CV are all examples of your personal data, if they identify you.

The University is a "controller" of your personal data. This is a legal term – it means that we make decisions about how and why we process your personal data and, because of this, we are responsible for making sure it is used in accordance with data protection laws.

This information should be read together with the notices attached to the various parts of the application form and selection process. It does not form part of any contract and may be updated from time to time.

A separate privacy notice is used and issued to you if you become employed or work for the University.

2. DATA PROTECTION PRINCIPLES

We will comply with data protection law, which states that personal data we hold about you must be:

1. Used lawfully, fairly and in a transparent way
2. Collected only for valid and lawful purposes that we have clearly explained to you
3. Relevant to the purposes we have told you about and limited only to those purposes
4. Accurate and up-to-date
5. Kept only as long as necessary for the purposes we have told you about
6. Processed and kept securely
7. Used in accordance with principles of accountability and compliance

3. WHAT INFORMATION DO WE COLLECT ABOUT YOU?

We cannot administer our recruitment procedures without your personal data. We will collect, store and use the following categories of information about you at various stages of the recruitment process:

- Personal contact details such as name, title, addresses including home address, personal email address, telephone numbers
- Date of birth
- Gender
- Professional and educational details – details of your qualifications, skills, experience, employment history, professional memberships and information about your current employment including your employer name, place of work, job title, pay and line manager
- Information about your entitlement to work in the UK – nationality and copies of your passport and/or visa and other documents evidencing your proof of address and identity
- Information about any disability you wish to declare so that we can make any “reasonable adjustments” that would assist you at interview
- Equality monitoring information – including information about your age, ethnic origin, sexual orientation, disability, religion or belief
- Details of unspent criminal convictions – details of unspent criminal convictions or cautions
- CCTV footage in some parts of the University campus

4. HOW DO WE COLLECT PERSONAL INFORMATION ABOUT YOU?

We collect this information in a variety of ways. For example:

- You provide us with personal data when you apply for a job with us, when you complete our application forms, send us your CV/personal statement or correspond with us. Data may be collected through interviews or other forms of assessment such as presentations or tests.
- From recruitment agencies, where you apply for a job in this way.
- Data may be obtained from your passport or other identity documents.
- If you are offered a role, information about you or your previous employment may be collected from third parties, such as references supplied by other organisations you have worked for and - for relevant roles - information from criminal records checks. We will normally seek information from third parties only once a job offer has been made to you.
- We receive information from our Occupational Health provider regarding any medical condition you have declared to them and any reasonable adjustments recommended, for which we would need to be aware, in respect of your job role with us.

Data is stored in a range of different places, including in the recruitment portal, in emails and in our HR management systems.

5. HOW DO WE USE YOUR PERSONAL DATA?

Under the General Data Protection Regulation (GDPR), we are only allowed to use personal information if we have a proper reason or ‘legal basis’ to do so.

In most cases, we need this personal data in order to:

- Comply with a legal obligation (for example to check your right to work in the UK), or
- Potentially enter into an employment contract or agency worker agreement with you.

We will use your data to administer your job application and make a decision about your suitability for the post you have applied for.

We may also convert your personal data into statistical or aggregated form so that you are not identified or identifiable from it in order to conduct research and analysis and produce statistical research and reports.

6. HOW WE USE PARTICULARLY SENSITIVE PERSONAL DATA

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 data.

We process special categories of personal data for purposes of equality monitoring and reporting including race and ethnic origin, sexual orientation, politics, religion or belief and disability. We aggregate or depersonalise this data on job applicants for analysis and reporting purposes so you will not be identified. Our equality monitoring process is designed to allow you to select 'prefer not to say' for categories that you do not wish to provide information. There is no detrimental effect on your application if you choose this option for the special categories of data.

The UK Data Protection Act 2018 adds information about criminal allegations, proceedings or convictions to the list of special categories compiled under the GDPR. We only use criminal record data when the law allows us to do so, e.g. where it is necessary to carry out our obligations and exercising specific rights under employment law and where it is necessary for the prevention and detection of crime or fraud. We consider at the point an offer of employment is made whether any criminal record information would make you unsuitable for the type of work to be completed.

We use data relating to health in order to make any adjustments you require during the recruitment and selection process and also to determine your suitability for a post for which you have applied.

7. AUTOMATED DECISION-MAKING

We do not use automated decision-making as part of our recruitment process.

8. DATA SHARING: WHO HAS ACCESS TO YOUR DATA?

Your personal information will be accessed and processed by authorised staff (i.e. line managers, recruitment panels, HR professionals and occupational health professionals) who are involved in the management and administration of the recruitment process and have a legitimate need to access your information for certain specific purposes, such as:

- Recruitment and HR teams – administering the recruitment process
- Line managers & recruitment panels – assessing your suitability for a job

Any sensitive data you provided as part of the equalities monitoring form or for the purpose of the guaranteed interview scheme are only viewed by HR staff. The data is used only for monitoring purposes and is not shared with the recruiting manager or panel members.

We will share your personal data with and request information about your personal data from previous employers to complete the reference checking process.

Third parties who process data on the University's behalf

We have agreements with third party service providers who provide specialist services on our behalf, e.g.

- Recruitment agencies (where applicable)
- The provider of the e-recruitment system
- The Occupational Health Provider
- Lawyers who provide employment law advice to the University
- The Disclosure and Barring Service (DBS) to obtain necessary criminal records checks

These third parties will process personal information in accordance with our instructions and make decisions regarding the information as part of the delivery of their services; they are also required to put in place appropriate security measures that ensure an adequate level of protection for personal information.

9. HOW DO WE KEEP YOUR DATA SECURE?

We take the security of your data seriously. We have internal policies and technical measures in place to safeguard your personal information.

Access to systems that hold employment related information is restricted to authorised personnel through the use of unique identifiers and passwords. Your information is stored on systems that are protected by secure network architectures and are backed-up on a regular basis for disaster recovery and business continuity purposes and to avoid the risk of inadvertent erasure or destruction.

Third parties will only process your data on our instructions and where they have agreed to treat the information confidentially and keep it secure.

We will not transfer your data outside the European Economic Area (EEA). If you are located outside the EEA and we need to transfer data in order to you in order to carry out the selection or recruitment process, we will only transfer data with your explicit consent.

10. DATA RETENTION – FOR HOW LONG DO WE KEEP YOUR DATA?

If you are not successful in obtaining a role with the University, your personal data will remain on file for one year from the end of the application process.

If you are successful in obtaining a role with the University, your personal data will remain on file for the duration of your employment and for six years after the end of your employment. The employee privacy notice gives further information about how data is processed for employees, workers and contractors.

We hold your personal data after a recruitment process in order to:

- Respond to correspondence, concerns or complaints
- Establish and defend any legal rights

We may also retain data that has been made anonymous for monitoring and reporting purposes. It will not be possible to identify you from such data.

11. YOUR RIGHTS

Under the GDPR, you are entitled to:

- **Request access** to the personal information that we hold about you.
- **Request correction** of the personal data that we hold about you, if you think it is inaccurate or incomplete.
- **Request erasure** of your personal data – you can ask us to delete it if you do not think we have a good reason to continue to process it or if you have exercised your right to object to processing.
- **Object to processing** of your personal data:

Where our processing of your personal data is based on your consent, you have the right to withdraw your consent at any time. If you do decide to withdraw your consent we will stop processing your personal data for that purpose, unless there is another lawful basis we can

rely on – in which case, we will let you know. Withdrawal of your consent will not impact any of our processing up to that point.

Where our processing of your personal data is necessary for our legitimate interests, you can object to this processing at any time. If you do this, we will need to show either a compelling reason why our processing should continue, which overrides your interests, rights and freedoms or that the processing is necessary for us to establish, exercise or defend a legal claim.

- **Request the restriction of processing**, e.g. if you want to check that it is accurate or find out why we are processing it.
- **Request the transfer** of your personal information to another party and/or receive a copy in a format that you can easily re-use for your own purpose(s).

If you would like to exercise any of these rights, please contact the University's Data Protection Officer gdpr@stmarys.ac.uk.

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

If you believe that the organisation has not complied with your data protection rights, you can complain to the Information Commissioner <https://ico.org.uk/>

12. WHAT IF YOU DO NOT PROVIDE PERSONAL DATA?

You are under no statutory or contractual obligation to provide us with data during the recruitment process. However, if you do not 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.

13. UPDATES TO THIS NOTICE

We may update this notice from time to time to reflect changes to the type of personal data that we process and/or the way in which it is processed. We will notify you of any material changes to this notice during the recruitment process.

Date of approval and issue	14.05.19
Document version and date	V1.1 – 09.04.19
Review date	May 2020
Document owner/s	HR Operations Manager Data Protection Officer
