St Mary's University Twickenham London

Data Protection Policy

Contents

1. INTRODUCTION

St Mary's University is committed to complying with the General Data Protection Regulation ("GDPR") which came into force on 25 May 2018.

The University will take all reasonable steps necessary to ensure that personal data not in the public domain is secure from unauthorised or unlawful processing and accidental loss, damage or destruction.

This Policy sets out how St Mary's University handles the Personal Data of our students, employees, workers, suppliers and other third parties.

This Policy applies to all Personal Data we process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

This Policy applies to all University Personnel. You must read, understand and comply with this Policy when processing Personal Data on behalf of the University and attend training on its requirements.

Your compliance with this Policy is mandatory. Related policies and privacy guidelines are available to help you interpret and act in accordance with this policy. You must also comply with all such related policies and privacy guidelines. Any breach of this policy may result in disciplinary action.

SCOPE

We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times.

The University is exposed to potential fines of up to EUR20 million (approximately £18 million) or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the GDPR.

All members of the Senior Management Team and Department Heads are responsible for ensuring all University Personnel comply with this policy and need to implement appropriate practices, processes, controls and training to ensure such compliance.

2. DEFINITIONS:

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

University Personnel: all employees, workers, students, contractors, agency workers, consultants, directors, members and others.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Data Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. **We are the Data Controller of all Personal Data** relating to our University Personnel and Personal Data used in our business for our own commercial purposes.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.

Data Protection Officer (DPO): the person required to be appointed in specific circumstances under the GDPR. Where a mandatory DPO has not been appointed, this term means a data protection manager or other voluntary appointment of a DPO or refers to the University data privacy team with responsibility for data protection compliance; this is the Clerk to the Board of Governors.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

General Data Protection Regulation (GDPR): the General Data Protection Regulation (*(EU) 2016/679*). Personal Data is subject to the legal safeguards specified in the GDPR.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Guidelines: the University privacy/GDPR related guidelines provided to assist in interpreting and implementing this Policy and Related Policies.

Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies: separate notices setting out information that may be provided to Data Subjects when the University collects information about them. These may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Related Policies: the University's policies, operating procedures or processes related to this Policy and designed to protect Personal Data.

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

3. PRINCIPLES OF GDPR

The University is required to process personal data according to the principles which are set out in the GDPR.

Principles	The context for the University
Lawfulness, Fairness and Transparency	The University explains to its staff, students and customers how it processes personal data at the point of collection and for what purposes
Purpose limitation	The University only uses the personal data it has for the purposes it was collected
Data Minimisation	The University only collects personal data which is relevant to the purposes it is required
Accuracy	The University ensures that the data is correct, up to date and able to be rectify any mistakes quickly
Storage Limitation	The University does not retain personal data for longer than it is necessary
Integrity and Confidentiality	The University protects its personal data against unauthorised access, loss or destruction by a range of security measures

A new accountability principle requires us to be able to **evidence compliance** with these principles.

4. PERSONAL DATA

The GDPR defines personal data as:-

'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a **name, an identification number, location data, an online identifier** or to one or more factors specific to the **physical, physiological, genetic, mental, economic, cultural or social identity** of that natural person.'

Sensitive personal data is classed as:-

'special categories' data, including racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.'

In order to lawfully process special category data, you must identify both a lawful basis under Article 6 (set out in paragraph 5.1.1) and a separate condition for processing special category data under Article 9 (set out in paragraph 5.1.2). These do not have to be linked.

5. LAWFULNESS

5.1 LEGAL BASIS FOR PROCESSING PERSONAL DATA

In order for it to be legal and appropriate for the University to process personal data, at least one of the following conditions must be met:

- **Consent:** The data subject has given clear consent to process their personal data for a specific purpose.
- **Contract**: The processing is required due to a contract
- **Legal Obligation**: the processing is necessary in order to comply with the law
- **Vital Interests**: It is necessary to protect someone's vital interests (i.e. life or death situation)
- **Public Task**: It is necessary for the performance of a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- **Legitimate Interests**: the processing is necessary for your legitimate interests or the legitimate interests of a third party *unless* there is a good reason to protect the individual's personal data which overrides those legitimate interests.

5.2 PROCESSING OF SENSITIVE PERSONAL DATA

Special Category Personal Data:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data for the purpose of uniquely identifying a natural person
- health conditions
- sexual life or sexual orientation
- personal data relating to criminal convictions and offences

The processing of sensitive personal data by the University must be based on both a legal base and one of the following:

Legal Basis (Sensitive personal data)	Examples
the Data Subject has given **Explicit Consent**	• A signature from the data subject • A tick in an unchecked box by the data subject to say 'I consent' • An oral statement 'Yes, I agree'
necessary for complying with **employment or social security law**	• Sickness absence, Notifying the University of Trade • Union membership; • Changing an employee's contract to part-time after an illness.
necessary to protect the **vital interests** of the data subject	• Where the data subject is physically or legally incapable of giving Consent • Being unconsciousness, medical data can be provided to the paramedics.
the processing relates to personal data which are **manifestly made public** by the data subject	• Alumni research, honorary degrees, ethical donatio ns • Assessment; • A media interview published in a newspaper or broadcast on TV.
necessary for the purposes of **preventive or occupational medicine,** for the assessment of the working capacity of the employee	• Occupational therapy assessments
reasons of public interest in the area of public health, provided it is subject to professional confidentiality	in cases of threats to health from infectious diseases and this a duty to notify to prevent the spreas of the disease
archiving, research or statistical purposes if it is subject to certain safeguards (i.e. pseudonymisation or anonymisation, the research is not carried out for the purposes of making decisions about particular individuals and it must not be likely to cause substantial damage/distress to an individual.	• Analysis and reporting of equality and diversity information

Further University examples of processing sensitive personal data:

1. Details of relevant unspent convictions for the purposes of assessing eligibility to enrol on the University's academic programmes

2. Details of relevant unspent convictions for the purposes of recruiting relevant staff

3. checks conducted by the Disclosure and Barring Service for the purposes of assessing eligibility of staff or students to engage in work with children and vulnerable adults, as permitted by legislation relating to the rehabilitation of offenders or for determining fitness to practise relevant professions

4. Unspent convictions o**r** allegations of sexual misconduct for staff and student disciplinary purposes

5. health data for the purposes for assessing eligibility to undertake relevant professional programmes, assessing fitness to study or to engage in University activities or for assessing fitness to work/occupational health

6. Details of disability for the purposes of assessing and implementing reasonable adjustments to the University's policies, criteria or practices

7. Details of racial/ethnic origin, sexual orientation, religion/belief for the purposes of equality monitoring

6. DATA SUBJECT'S RIGHTS AND REQUESTS

Data Subjects have rights when it comes to how we handle their Personal Data. These include:

Right	University Context
Right to be informed	The right to be informed about the collection and use of their personal data, including the purpose, retention period, and who it will be shared with - covered by the **Privacy Notice.**
Right of access	The right to access their personal data and be aware of and verify the lawfulness of the processing.
Right to rectification	The right to have inaccurate personal data rectified or completed (if incomplete). If the personal data has been shared with third parties, or within the University, they must be contacted and informed of the rectification - unless this proves impossible or involves disproportionate effort.
Right to erasure / right to be forgotten	The right to have personal data erased (or 'the right to be forgotten'); this is not absolute, however, and will only occur in very limited circumstances in the University context.
Right to restriction of processing	The right to request restriction or suppression of their personal data; again, this only applies in certain circumstances and you are still permitted to store the data.
Right to data portability	The right to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. Certain requirements have to be met.
Right to object	The right to object to processing based on legitimate interests, direct marketing, and processing for purposes of scientific/historical research and statistics – unless certain conditions are met.
Automated decision making, including profiling	Profiling is the processing of data to evaluate, analyse or predict behaviour or any feature of their behaviour, preferences or identity. Individuals have the right not to be subject to decisions based solely on automated processing. When profiling is used, measures must be put in place to ensure security and reliability of services. Automated decision-taking based on sensitive data can only be done with explicit consent.

The availability of rights depends on the legal justification for processing and there may be instances where these may not be accommodated. The table below summarises when rights are and are not available:-

Legal Justification	**The Right to:**				
	Object	Erasure	Automated decision making	Rectification	Portability
Consent	X but can withdraw consent	✓	X but can withdraw consent	✓	✓
Contract	X	✓	X	✓	✓
Legal Obligation	X	X	X	✓	X
Vital Interest	X	✓	X	✓	X
Public Task	✓	X	✓	✓	X
Legitimate Interest	✓	✓	✓	✓	X

Subject Access Request

You must verify the identity of the individual requesting this data and immediately forward the request to your supervisor and the DPO (Clerk to the Board of Governors) and comply with the University's Data Subject response process. Do not disclose Personal Data to third parties without proper authorisation.

Time Limit
Requests must be complied to within one month of receipt.

Fees
A fee cannot be charged to comply with a subject access request. However, where the request is manifestly unfounded or excessive you may charge a "reasonable fee" for the administrative costs of complying with the request. A reasonable fee may also be charged if an individual requests further copies of their data following a request.

7. COMPLIANCE

The University must have adequate resources and controls in place to ensure and to document GDPR compliance including:

(a) appointing a DPO (the Clerk to the Board of Governors) and an executive accountable for data privacy;

(b) implementing Privacy by Design when Processing Personal Data and completing DPIAs ;

(c) integrating data protection into our policies and procedures, in the way personal data is handled by us and by producing required documentation such as Privacy Notices, Records of Processing and records of Personal Data Breaches;

(d) training staff on compliance with Data Protection Law and keeping a record accordingly; and

(e) regularly testing the privacy measures and conducting periodic reviews and audits to assess compliance.

8 RECORD KEEPING

The GDPR requires us to keep full and accurate records of all our data Processing activities.

You must keep and maintain accurate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents.

These records should include:

- the name and contact details of the Data Controller and the DPO
- clear descriptions of the Personal Data types
- Data Subject types
- Processing activities
- Processing purposes
- third-party recipients of the Personal Data
- Personal Data storage locations
- Personal Data transfers
- the retention period and a description of the security measures in place.

Data maps should be created which should include the detail set out above together with appropriate data flows.

9. The Data Protection Officer

The Data Protection Officer ("DPO") is responsible for overseeing this policy and developing related policies and privacy guidelines. That post is held by the Clerk to the Board of Governors and Company Secretary.

The DPO can be contacted on:-

Email: gdpr@stmarys.ac.uk
Telephone: 020 8240 4267

Please contact the DPO with any questions about the operation of this Policy or the GDPR or if you

have any concerns that this Policy is not being or has not been followed.

The DPO must always be contacted in the following circumstances:-

Circumstances
Lawfulness Unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by the University)
Consent You need to rely on Consent and/or need to capture Explicit Consent
Privacy Notes You need to draft Privacy Notices or Fair Processing Notices
Retention Unsure about the retention period for the Personal Data being processed
Protecting Data Unsure about what security or other measures you need to implement to protect Personal Data
Personal Data Breach
Transferring Data Unsure on what basis to transfer Personal Data outside the EEA
Data Subject's Requests You need any assistance dealing with any rights invoked by a Data Subject
New Reasons for Data Processing Engaging in a new, or change in, processing activity which is likely to require a DPIA or plan to use Personal Data for purposes others than what it was collected for
Automated Processing Undertaking activities involving Automated Processing including profiling or Automated Decision-Making
Direct Marketing Require help complying with applicable law when carrying out direct marketing activities
Third Parties Require help with contracts or other areas in relation to sharing Personal Data with third parties (including vendors)

10. REPORTING A DATA BREACH

The GDPR requires Data Controllers to notify any Personal Data Breach to the Information Commissioner and, in certain instances, the Data Subject.

A personal data incident can occur for a number of reasons some examples of these include:

- Loss or theft of data or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Unauthorised disclosure (e.g. email sent to incorrect recipient or document posted to the wrong address or personal information posted onto the website without consent)
- Human error;
- Unforeseen circumstances such as a fire or flood;
- Hacking attack;
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it.

A data breach must be reported to the Data Protection Officer immediately.

The Information Commissioner's Office shall be notified within 72 hours of the breach where there is a risk to the rights and freedoms of individuals such as discrimination, discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay

We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. **Immediately contact the Data Protection Officer** -you should preserve all evidence relating to the potential Personal Data Breach.

11. TRAINING AND AUDIT

We are required to ensure all University Personnel undergo adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

All University Personnel must undergo all mandatory data privacy related training and ensure your team undergo similar mandatory training in accordance with the University's mandatory training guidelines.

You must regularly review all the systems and processes under your control to ensure they comply with this policy.

12. PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENT (DPIA)

It is important to consider privacy issues when considering **new processing** activities or setting up **new procedures or systems** that involve personal data. GDPR imposes a specific 'privacy by design' requirement emphasising the need to implement appropriate technical and organisational measures during the design stages of a process and throughout the lifecycle of the relevant data processing to ensure that privacy and protection of data is not an after-thought

You must assess what Privacy by Design measures can be implemented that Process Personal Data by taking into account the following:

(a) the state of the art;

(b) the cost of implementation;

(c) the nature, scope, context and purposes of Processing; and

(d) the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

Data controllers must also conduct DPIAs in respect to high risk Processing.

New projects involving personal data are required to carry out a privacy impact assessment to identify privacy risks and plan appropriate mitigation. These can include:

(i) use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

(ii) Automated Processing including profiling and ADM;

(iii) large scale Processing of Sensitive Data; and

(iv) large scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

(a) a description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate;

(b) an assessment of the necessity and proportionality of the Processing in relation to its purpose;

(c) an assessment of the risk to individuals; and

(d) the risk mitigation measures in place and demonstration of compliance.

13. AUTOMATED PROCESSING (INCLUDING PROFILING) AND AUTOMATED DECISION-MAKING ("ADM")

This relates to automated decisions or profiling that could result in significant affects to an individual. Profiling is the processing of data to evaluate, analyse or predict behaviour or any feature of their behaviour, preferences or identity. Individuals have the right not to be subject to decisions based solely on automated processing. When profiling is used, measures must be put in place to ensure security and reliability of services. Automated decision-taking based on sensitive data can only be done with explicit consent.

ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

(a) a Data Subject has Explicitly Consented;

(b) the Processing is authorised by law; or

(c) the Processing is necessary for the performance of or entering into a contract.

We must also inform the Data Subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

A DPIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

14. DIRECT MARKETING

We are subject to certain rules and privacy laws when marketing to our customers.

A Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be **explicitly offered** to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information. The University must cease direct marketing activity if an individual requests the marketing to stop.

15. SHARING PERSONAL DATA

Personal Data cannot be shared with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the Personal Data we hold with another employee, agent or representative of our group (which includes our subsidiaries and our ultimate holding University along with its subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

You may only share the Personal Data we hold with third parties,(e.g. our service providers) if:

(a) they need to know the information for the purposes of providing the contracted services;

(b) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

(c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

(d) the transfer complies with any applicable cross border transfer restrictions; and

(e) a fully executed written contract that contains GDPR approved third party clauses has been obtained.

16. TRANSFERRING DATA OUTSIDE THE EEA

The GDPR restricts data transfers to countries outside the EEA.

International data transfer includes:

- Sending personal data from the University to an organisation, company or an individual that is based in a non-EEA country.
- Remotely accessing a University database from your computer if at that time you are in a non-EEA country.

You may only transfer Personal Data outside the EEA **if one of the following conditions applies**:

(a) the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms; The countries currently approved can be found here:

https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

(b) appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;

(c) the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or

(d) the transfer is necessary for one of the other reasons set out in the GDPR including:

- the performance of a contract between us and the Data Subject,
- reasons of public interest,
- to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

CHANGES TO THIS POLICY

The University reserves the right to change this Policy at any time so please check back regularly to obtain the latest copy of this Policy. This Policy does not override any applicable national data privacy laws and regulations in countries where the University operates.

LINKS TO FURTHER INFORMATION

Information Commissioners Office: https://ico.org.uk/

GDPR Intranet Site: http://staffnet/Governance/Pages/GDPR.aspx

GDPR Handbook

DPIA Template

LIA Template

Document title	Data Protection Policy							
Author (name/role)	Andrew Browning, Clerk to the Governors, Sukhi Panesar, Senior In-House Legal Advisor							
Document date	July 2018							
Effective from								
Equality Impact Assessment (EIA) completion date								
History (where discussed/who circulated to/committees)	GDPR Working Group, SMT							
Approval body and date								
Review date including EIA	2021							
Document posted (specify Yes, No, N/A)	Website		StaffNet		SIMMSpace		simmsCAPital	