St Mary's University Twickenham London

Data Protection Policy, 2015/16

St Mary's University is committed to the implementation of the Data Protection Act 1998 which came into force on 1 March 2000 and thereby the protection of individual rights to privacy with respect to the processing of personal data.

The University will take all reasonable steps necessary to ensure that personal data not in public domain are secure from unauthorised or unlawful processing and accidental loss, damage or destruction. It will process the data in accordance with current legislation and the University's Data Protection Notification and will not disclose the information to any unauthorised third party.

Definitions of data protection terms are attached at Appendix A.

1 Responsibility for Data Protection

1.1 Data Protection Officer

The Registrar is the University Data Protection Officer. The Registrar is responsible for dealing with day-to-day data protection matters and for developing good practice across the University and advising staff on compliance with the Act.

Any questions or concerns about the interpretation or operation of this policy should be taken up initially with the Registrar.

1.2 Board of Governors

The University as a body corporate is the data controller under the new Act and the Board of Governors is ultimately responsible for implementing the Data Protection Act.

1.3 Senior Staff and Heads of Services

Senior Staff, Heads of Schools and Services and all in line- management roles have the responsibility of ensuring compliance with this policy and developing and encouraging good practice in regards to handling personal data within their areas.

1.4 Members of the University Community

This policy applies to all members of the University including visiting lecturers and other associate members, students and data processors. Although it does not form part of the formal contract of employment or the regulations for being a student, it is a condition of employment or being a student that members of the University will abide by the rules and policies made by the University from time to time. Any breach of the data protection policy or the Data Protection Act 1998 will be considered as a breach of discipline and existing disciplinary proceedings will apply.

2 The Scope of the Policy

This policy applies to **all** personal data held by the University, whether on computer, microfiche, paper, email or other storage method. Personal data is information about staff, students and other living individuals including their personal characteristics, who is identifiable by the information, or who could be identified by the information combined with other data.

Personal data covers both facts and opinions about the individual. It also includes information regarding the intentions of the University towards the individual, although in some limited circumstances exemptions will apply.

Particular restrictions are placed on sensitive personal data which is personal data consisting of information as to:

- racial and ethnic origin;
- political beliefs;
- religious beliefs or other beliefs of a similar nature;
- trade union membership;
- physical or mental health or other medical conditions;
- sexual life;
- commission or alleged commission of any offence;
- any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

3 Personal Data held by the University

The University needs to hold information about employees, students and other users to allow it operate efficiently and effectively. Such information will, however, be collected and used fairly, stored safely and securely and not be disclosed to any third party unlawfully.

4 Processing Personal Data

Any member of staff processing personal data must comply with the eight enforceable principles under the act so that the data is:

- fairly and lawfully processed;

- processed for limited purposes;
- adequate, relevant and not excessive;
- accurate;
- not kept longer than necessary;
- processed in accordance with the data subject's rights;
- secure;
- not transferred to countries without adequate protection.

In addition they must ensure that the conditions applied by the Act to the processing of personal data are observed so that:

- the individual has given their explicit consent to it being processed
- it is necessary for the performance of a contract; or
- it is necessary to comply with a legal obligation of the University; or
- it is necessary in order to protect the **vital** interests of the individual.

Where sensitive data is being processed at least two of the above conditions must be met.

5 Collecting, Handling and Holding Personal Data

Staff may only collect information about other people if they are authorised to do so as part of their University responsibilities. When doing so staff must comply with the guidelines for handling personal data.

Under this policy, all staff who collect hold or handle personal data are responsible for ensuring that:

- data subjects are aware of the details and purpose of any personal data collected;
- any personal data which they hold is kept securely;
- personal information is not disclosed either orally or in writing; or accidentally or otherwise to any unauthorised third party.

Staff should note that unauthorised disclosure will usually be considered as a disciplinary matter, and may be considered gross misconduct in some cases.

Personal data should be:

- in a secure office; or
- kept in a locked filing cabinet; or
- in a locked drawer; or
- if it is computerised, be password protected; or kept only on disk which is itself kept securely.

6 Research Projects

Staff and students may only collect personal data as part of a research proposal for which they have prior and explicit ethical approval given by the

Ethics Committee. Students who are collecting personal data must abide by this policy.

7 Responsibilities of Staff/Students as Data Subjects

For the purposes of processing their employment/ being a student all staff and students are responsible for:

- checking that any information that they provide to the University in connection with their employment/ their studies is accurate and up to date;
- informing the University of any changes to information, which they have provided. i.e. changes of address, telephone number and next of kin;
- checking the information that the University will send out from time to time, giving details of information kept and processed about them;
- informing the University of any errors or changes.

The University cannot be held responsible for any errors, unless the staff member/student has informed the University in writing of these errors.

8 Collection Notices

The University will provide staff and students, alumni and other users of University services with a collection notice of the personal data that they collect and the uses for which it is held. It will also provide opportunities for staff, students and alumni to check and update such information on a regular basis.

9 Publication of University Information

The University places certain personal data it holds within the public domain. Personal data in the public domain is data which will be publicly available, and may be disclosed to third parties without recourse to the individual. Information in the public domain is outlined in the University's Publication Schedule produced under the requirements of the Freedom of Information Act.

Information which is not in the public domain, and must not therefore be published, may only be processed in accordance with the conditions for processing outlined above.

10 Refusal of Consent

Where information is placed in the public domain, individuals must be given the opportunity to withhold their consent from its publication. Those responsible for publishing the data must have a procedure to enable this process of withholding consent. It should be noted, however, that staff and the University office that they hold will normally be deemed in the public domain.

11 Publication of Staff Information on the University Internet Site

Where such data is made available on the University website such information is potentially freely available worldwide. The University will only place contact details and other relevant staff information on the World Wide Web following their explicit consent unless it is related to a particular responsibility where it will be made clear that such details are in the public domain.

12 Student Data on the University Intranet

Student data is made available to staff via the Intranet to enable them to undertake their work. Such data will be only available via machines on campus and staff will only be able to have access relevant to their University employment responsibilities. Such access will be restricted by password and governed by the University policies on Internet security.

13 Disclosure of Data not in the Public Domain

Personal data which is collected by the University but is not in the public domain will remain private between the University and the data subject unless one or more of the conditions for processing as specified in the Act and outlined in 4 above applies.

14 Subject Consent

14.1 Staff Members

In order that the University can process details of a member of staff's employment and also operate effectively, it will need to collect and process personal data, including some sensitive personal data. Such data will be processed in accordance with the Act and only used for the purposes provided.

All prospective staff will be asked to provide consent regarding particular types of information as outlined in the collection notice when an offer of employment is made. A refusal to sign such a form can result in the offer of employment being withdrawn.

Where further data is collected during a member of staff's employment, they will be informed of this and asked to provide consents where necessary.

14.2 Students

All students will be asked to sign a Registration Form which will include a declaration giving consent to the processing of their personal data in accordance with the student collection notice. They will be provided with a collection notice which will explain what data is required and for what purpose. Where further data is collected during a student's studies, they will be informed of this and asked to provide consents where necessary.

14.3 Alumni and Users of University Services

Former students wishing to be a member of the University alumni or others who use the University' s services such as the Conference Office will be required to provide the necessary data in order for such services to be able to operate. They will be provided with a collection notice which will state what data is being collected and what it will be used for.

15 References

Staff and students have the right to see references written about them either internally or externally. Where such references were provided prior to the implementation of the 1998 Data Protection Act and were believed to be in confidence, this data will not be released without the prior permission of the referee.

16 Retention of Data

An information retention schedule is attached at Appendix 2.

16.1 Staff Data

Personal data relating to members of staff will only be retained by the University for such time as is necessary under the statute of limitations. A record of the staff name, sufficient identifying data and their employment record will, however, be kept in perpetuity.

16.2 Student Data

Personal data relating students will only be retained by the University for such time as is necessary under the statute of limitations. A record of the student, sufficient identifying data and their study record will, however, be kept in perpetuity.

16.3 Alumni and Other Users' Data

Data on alumni will be retained on the alumni database. The data for other users of University services will be kept for such time as is necessary under the statute of limitations.

17 Data Subject Access Rights

Staff, students and other users of the University have the right to access any personal data that is being kept about them. In general, the University will normally make data available, such as the personnel file or the student's record. Any member of staff or student who wishes to access other information should write to the Data Protection Officer with details of their request. Any request must include information which may be required by the Data Protection Officer in order to locate the information requested. The University will make a charge of £I0 on each occasion that access is requested.

The University aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within the statutory timeframe of 40 days for Data Subject Access Requests, unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the data subject making the request.

University staff should note that they may not have access to data that is collected for the purposes of management planning or forecasting.

18 University Undertaking Regarding the Use of Personal Data

The University does not sell trade or rent personal data to others.

19 Closed Circuit Television

The University operates a closed circuit television (CCTV) system which monitors certain areas of the University. The system has been installed to reduce the fear of crime and to provide a feeling of safety in public areas. The images shown and recorded by the system are kept in accordance with the 1998 Data Protection Act and are governed by the CCTV Code of Practice which is available from the Security Lodge.

20 The Use of Cameras and Audio Recording Equipment by University Security Staff

University Security Staff are now equipped with body cameras in order to enhance the monitoring of incidents of crime, the protection of students and staff, and the follow-up support for any internal disciplinary and/or external Police proceedings.

The images and audio recorded by the system are kept in accordance with the 1998 Data Protection Act and are governed by the CCTV Code of Practice which is available from the Security Lodge.

21 Using University Resources for Personal Use

Staff and students may not process or hold personal data on other individuals for any purpose not related to their work. Staff and students who undertake such activity will be dealt with under the disciplinary code.

Tam Milner
Registrar

Appendix 1

DATA PROTECTION DEFINITIONS

Data	Any information which is being processed automatically or recorded as part of a relevant filing system
Data Controller	The individual/organisation responsible for ensuring the requirements of the Data Protection Act 1998 are complied with
Data Subject	An individual who is the subject of personal data
Personal Data	Data which relate to a living individual who can be identified from those data or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller. Personal data include any expression of opinion about the individual and any indication of the intentions of the data controller
Processing	Accessing, altering, adding to, deleting, changing, disclosing or merging data and anything else which can be done with data
Relevant Filing System	Any paper filing system or other manual filing system which is structured so that information about an individual is readily accessible: i.e. structured by reference to individuals (e.g. alphabetical), by reference to criteria relating to individuals, by numerical reference (e.g. student number) etc.
Sensitive Data	Information about an individual's racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health or condition, sexual life, commission or alleged commission of any offence, any proceedings for any offence committed or alleged to have been committed by him/her
Third Party	Any individual/organisation other than the data subject, the University and/or its servants and/or agents

Please note that the above definitions have been simplified and are not definitive.

Appendix 2

Guidelines for Retention of Personal Data

This is not an exhaustive list and those responsible for Finance, Personnel and Registry should ensure that it is updated as required by changes in the law, new regulations or new practices.

Type of Data	Suggested Retention Period	
Personnel files including training records and notes of disciplinary and grievance hearings.	6 years from the end of employment	References and potential litigation
Application forms/interview notes	At least 6 months from the date of the interviews.	Time limits on litigation
Facts relating to redundancies where less than 20 redundancies	3 years from the date of redundancy	As above
Facts relating to redundancies where 20 or more redundancies	12 years from date of redundancies	Limitation Act 1980
Claims for redundancy and long service	7 years after employment ceased	Statute of Limitations
Salary registers	6 years	Taxes Management Act
Expense accounts/records	7 years	Statute of Limitations and Taxes Management Act
Overtime records/authorisation	3 years	Commercial/audit
Income tax records for employees leaving i.e. P45	6 years	Taxes Management Act
Notice to employer of tax code and certificate of pay and tax deducted (P60)	6 Years	Taxes Management Act
Notice of tax code change	6 Years	Taxes Management Act
Annual return of taxable pay and tax deducted	6 years	Taxes Management Act
Records of pension deductions (including superannuation)	6 years	Pensions Act 1995
Copy pay slips	2 years	Commercial audit
Payroll and payroll control account	7 years	Statute of Limitations and Taxes Management Act
Staff personnel records	7 years after employment ceases	Statute of Limitations
Statutory Maternity Pay records and calculations	As Above	Statutory Maternity pay (General) Regulations 1986
Statutory Sick Pay records and calculations	As Above	Statutory Sick pay (General) Regulations 1982

Type of Data	Suggested Retention Period	
Accident books, and records and reports of accidents	3 years after the date of the last entry	RIDDOR 1985
Health records	During Employment	Management of Health and Safety at Work Regulations
Health records where reasons of termination of employment are connected with health, including stress related illness	3 years	Limitation period for personal injury claims
Medical Records kept by reason of the Control of Substances Hazardous to Health Regulations 1994	40 years	COSHHR 1994
Student records, including academic achievements, and conduct.	At least 6 years from the date the student leaves the HEI, in case of litigation for negligence, At least 10 years for personal and academic references, with the agreement of the student.	Limitation period for negligence
Examination Scripts	One year	For Appeals and assessment purposes
Computer Record	Indefinitely	
Student's file	Six years	
Appeals cases	Six years	