Data Protection Policy

From: Director of Legal Services **Date:** May 2018

1. Relevant Law

1.1 The General Data Protection Regulation (GDPR), will be incorporated into UK law via the Data Protection Act 2018. These are referred to in this policy as the Data Protection Legislation as defined in the **Glossary of Terms**.

1.2 Laws of Malaysia: Act 709: Personal Data Protection Act 2010

2. Introduction

2.1 The Data Protection Legislation is designed to both strengthen individual (**Data Subject**) rights in respect of Personal Data and to place greater obligations on those (**Data Controllers** and **Data Processors**) who process that **Personal Data**.

2.2 The University of Southampton (the University) is committed to protecting the rights and freedoms of individuals and complying with its obligations when processing Personal Data (either as a Data Controller or as a Data Processer).

2.3 This policy forms part of the University's Information Governance Framework and demonstrates compliance with its obligations under the **Data Protection Legislation**.

3. Scope

3.1 This policy applies to University of Southampton employees, students, agency staff, visitors, contractors and third parties (Users) who process Personal Data.

4. Aims

4.1 This policy is designed to inform Users of their obligations under the Data Protection Legislation and to set out the standards expected by the University in relation to the processing of Personal Data and safeguarding individuals' rights and freedoms.

5. Personal Data

5.1 The University holds Personal Data about Data Subjects such as employees, visitors, students, graduates, research subjects, patients and other third parties. Such Personal Data must only be processed in accordance with the principles of the Data Protection Legislation as set out in Schedule 1.

5.2 The University has taken steps to apply the principles of the Data Protection legislation to the processing of personal information to ensure compliance with the Data Protection Legislation. See the Application of the Data Protection Principles set out in Schedule 2.

6. Roles and Responsibilities

6.1 The Chief Information Officer undertakes the role of Senior Information Risk Owner ("SIRO") and has responsibility for reviewing the flows of Personal Data to understand whether Data transferred to external organisations flows outside of the UK.

6.2 The University's Data Protection Officer is responsible for highlighting data protection issues, reviewing flows of Personal Data with the SIRO, reporting any incidents, providing advice and training to University employees, monitoring compliance with the Data Protection Legislation and maintaining the currency of this policy.

6.3 The Caldicott Guardian is responsible for ensuring implementation of the Caldicott Principles set out in Schedule 3 with respect to patient-identifiable Personal Data.

6.4 All Users who are processing Personal Data are expected to read this policy and the **Data Breach Guidelines** set out in Schedule 4. They are expected to understand and apply the principles of the Data Protection Legislation set out in Schedule 1.

6.5 Users employed by the University and Users who are students at the University are expected to ensure that any Personal Data, which they process, is kept securely and that any personal information is not disclosed accidentally or otherwise to any unauthorised third party.

7. Confidentiality

7.1 The University is committed to protecting the confidentiality of those whose Personal Data it holds. Every User is bound by a legal common law duty of confidentiality and has an obligation to protect the Personal Data that they may come into contact with during the course of their work or study.

7.2 Users who are University employees are also bound by the confidentiality clause in their employment contract.

8. Student Users

8.1 A student of the University should only process Personal Data for an academic or University related purpose, with the knowledge and express consent of an appropriate University employee. The use of Personal Data by students should be limited to the minimum consistent with the achievement of academic objectives.

9. CCTV & surveillance systems

9.1 The University's CCTV and surveillance systems will be used in line with the University's **Surveillance Policy**.

10. Data Subject rights & privacy contacts

10.1 The Data Protection Legislation gives the Data Subject rights in respect of the Personal Data held about them by the University. These rights are set out in Schedule 5.

10.2 The University has introduced a **ServiceNow** platform to manage Data Subject requests for Personal Data to assist the University in meeting its timeliness and compliance obligations under the Data Protection Legislation.

10.3 Data Subject requests for access, rectification, erasure, portability and objections as to processing, to/of their Personal Data should be made through the University's website. Data Subject who are members of the University and have a University login and email account may submit their request via their University email account to: **data.protection@soton.ac.uk**.

10.4 All other requesters must upload and submit any supporting documentation verifying that they are the Data Subject or acting on behalf of the Data Subject through **Servicenow**. See Schedule 3 for a list of Data Subject rights.

10.5 For general enquiries about the University's Data Protection Policy and the Data Protection Legislation please contact:

The Data Protection Officer
Legal Services,
University of Southampton, Highfield
Southampton S017 1BJ
Telephone: (023) 8059 2400, e-mail: **data.protection@soton.ac.uk**

11. Disclosure

11.1 Users may not disclose any data about applicants, students or other employees, including information as to whether or not any person is or has been an applicant, student or employee of the University unless they are clear that they have been given authority by the University to do so. Particular care should be taken in relation to any posting of Personal Data on the internet.

11.2 No User may provide references to prospective employers, landlords or others without the consent of the Data Subject. It is therefore essential that where the University is given as a referee, the subject of the reference should provide the University with the necessary notification and consent.

11.3 No User may disclose Personal Data to the police or any other public authority unless that disclosure has been authorised by the University's Data Protection Officer.

12. Data retention

12.1 Personal Data must not be held for longer than necessary and it must be destroyed securely.

12.2 Personal Data should be reviewed periodically to check it is accurate and up to date and to determine whether retention is still necessary.

12.3 Appropriate measures must always be taken to ensure that the Personal Data that has been earmarked for destruction cannot be reconstructed and processed by third parties.

12.4 The University's Data Retention Schedule sets out the periods for which University business records will be held.

13. Data breaches

13.1 The University holds personal data on staff, students, alumni, research participants and other who are associated with the University. Users who access, hold or process personal including special category (sensitive personal data) for the purposes of conducting University business must take appropriate steps to ensure that no unauthorised or unlawful processing, accidental loss, destruction of or damage to personal data occurs.

13.2 If personal data including any special category data is unlawfully destroyed, lost, stolen, corrupted, disclosed or released to unauthorised persons notice must be given to the Data Protection Officer, the Chief Information Officer and the Head of Information Security immediately a data breach occurs, is threatened or is suspected.. This can be done by completing the Incident Report Form or telephoning +44 (0)23 8059 4684 during office hours and Security 02380592811 x22811 outside office hours.

13.3 The University has implemented the **Data Breach Guidelines** set out in Schedule 4 for all Users setting out the steps that must be taken in the event of a Personal Data breach.

14. Disciplinary consequences

14.1 Unlawful obtaining or disclosure of personal data (including the transfer of personal data outside the EEA) or any other breach of the Data Protection Legislation by Users will be treated seriously by the University and may lead to disciplinary action up to and including dismissal or expulsion and must be reported.

15. Monitoring compliance and review

15.1 All information governance and security policies and procedures will be subject to periodic audit and review to ensure that they remain fit for purpose and the University remains compliant.

16. Key policies and guidance

16.1 Key Information Governance policies, Glossary of Terms and guidance can be found **at** **Legal Services**.

17. Further information

17.1 Additional policies and guidelines concerning particular activities can be found at our Publication Scheme.

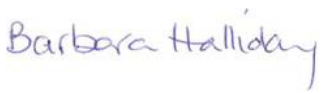
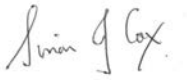
Document Control

File Name	Data Protection Policy
Original Author(s)	
Current Revision Author(s)	FTVB
Owner	Director of Legal Services
Publication Date	
Target Audience	

Version History

Version	Date	Author(s)	Notes on Revisions
00.01	May 2018	FTVB	

Document Sign Off

Name	Role	Doc version	Signoff date	Signature*
Barbara Halliday	Director of Legal Services	1	24-05-2018	
Professor Simon Cox	Chief Information Officer	1	24-05-2018	

*If signoffs are received by email, print names here and archive the sign off emails.
Add location of signoff emails here:

This is a controlled document. Whilst this document may be printed, the electronic version posted on the Intranet is the controlled document copy. Any printed copies of this document are not controlled.

Schedule 1: Data Protection Principles

1. Data Protection Principles

1.1 The following principles apply to all Users processing Personal Data. The term "processing" applies to all operations performed on the Personal Data during its life cycle including collection, storage, use and destruction.

1.2 Personal Data shall be:

1.2.1 Processed lawfully, fairly and in a transparent manner in relation to the Data Subject (**Principle 1: lawfulness, fairness and transparency**).

1.2.2 Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes (**Principle 2: purpose limitation**).

1.2.3 Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**Principle 3: data minimisation**).

1.2.4 Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (**Principle 4: accuracy**).

1.2.5 Kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed; Personal Data may be stored for longer periods insofar as the Personal Data is to be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Data Protection Legislation in order to safeguard the rights and freedoms of individuals (**Principle 5: storage limitation**).

1.2.6 Processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (**Principle 6: integrity and confidentiality**).

The University shall be responsible for, and be able to demonstrate compliance with, the above principles (**accountability**).

Schedule 2: Application of the Data Legislation Principles

2. Demonstrating Compliance

The University will apply the Data Protection Principles and the other requirements of the Data Protection Legislation to the management of all Personal Data throughout its life cycle by:

2.1 Collecting Personal Data

(Principle 1 -Lawfulness, fairness and transparency & Principle 2 -purpose limitation)

2.1.1 Only collecting and using personal data in accordance with a lawful basis;

2.1.2 Documenting each lawful basis we rely on for processing the Personal Data and have it available on request;

2.1.3 Using the Data Subject's Personal Data fairly for the purposes and in a way that they would reasonably expect;

2.1.4 Only relying on consent where the Data Subject has given their specific, informed and freely given consent, by way of a statement or clear affirmative action we can record and they can withdraw consent at any time without it being detrimental to them;

2.1.5 Informing Data Subjects of what we are doing with their Personal Data by way of privacy notices and other means. This information will include details of:

2.1.6 The identity, contact details and ICO registration number of the of the University and the Data Protection Officer,

2.1.7 What we are collecting,

2.1.8 The purposes we are collecting and using it,

2.1.9 What lawful conditions we rely on to process data for each purpose and how this affects their rights,

2.1.10 Whether we intend to process the data for other purposes and their rights to object,

2.1.11 Where we are getting their Personal Data from,

2.1.12 Whether we use automated decision making, including profiling and what impact this has on them and their rights to object,

2.1.13 Whether they need to provide Personal Data to meet a statutory or contractual requirement and if so, the consequences of not providing the data,

2.1.14 How we will keep their Personal Data secure,

2.1.15 Who we will share it with and why,

2.1.16 Whether it will be transferred outside of the UK or outside the EEA,

2.1.17 How long we retain their Personal Data,

2.1.18 What their rights are and how they can exercise them.

2.2 Holding/safeguarding/disposal of personal data

(Principle 4 - Accuracy, Principle 5 - storage limitation, Principle 6 - integrity & confidentiality)

2.2.1 Taking responsibility throughout the University for complying with the Data Protection Legislation,

2.2.2 Using appropriate technical and organisational measures to control access to Personal Data,

2.2.3 Requiring all Users who have access to personal data in the course of their work to complete basic data protection training, supplemented as appropriate by procedures and guidance relevant to their specific roles,

2.2.4 Enabling University employees and students to update their Personal Data to ensure accuracy,

2.2.5 Ensuring security standards are in place and are monitored,

2.2.6 Pseudonymising Personal Data wherever possible,

2.2.7 Anonymising Personal Data wherever necessary and appropriate, e.g. when using it for statistical purposes, so that individuals can no longer be identified.

2.2.8 Ensuring University employees can work securely away from University premises through secure systems and guidance,

2.2.9 Taking all reasonable steps to obtain assurance that all suppliers, contractors, agents and other external parties who process personal data for the University will comply with University policies and controls to protect Personal Data,

2.2.10 Embedding privacy by design and using data protection impact assessments to identify risks,

2.2.11 Recording and, where necessary, reporting data protection breaches,

2.2.12 Only collecting and disclosing minimum Personal Data for the minimum time necessary for the purpose,

2.2.13 Reviewing and updating our accountability measures at appropriate intervals,

2.2.14 Ensuring appropriate information governance and data protection policies are in place.

2.3 Processing of Personal Data (Principle 2 - purpose limitation)

2.3.1 Ensuring that if Personal Data is collected for one purpose it will not be reused for a different purpose that the Data Subject did not agree to or expect,

2.3.2 Ensuring that our processes are appropriately documented.

2.4 Disclosing and transferring personal data (Principle 6 - Integrity and confidentiality)

2.4.1 Maintaining data sharing agreements with educational partners and other external bodies with whom we may need to share personal data to deliver academic programmes, shared services or joint projects to ensure proper governance, accountability and control over the use of such data,

2.4.2 Ensuring that where the University is transferring personal data to another country outside the European Union appropriate agreements and auditable security controls to maintain privacy rights are in place,

2.4.3 Ensuring that our students are aware of how data protection law applies to their use of Personal Data in the course of their studies or research and how they can take appropriate steps to protect their own Personal Data and respect the privacy of others,

2.5 Destruction of personal data (Principle 5 - storage limitation)

2.5.1 Retaining University records in line with the Records Retention Schedule and only keeping Personal Data as long as is necessary.

2.5.2 Making appropriate and timely arrangements to ensure the confidential destruction of Personal Data in all media and formats when it is no longer required for University business.

3. Caldicott Principles

3.1 The University also holds Special Catagory Personal Data (medical/health data) about Data Subjects who are patients.

3.2 The following principles were devised by the Caldicott Committee in 1997 and represent best practice for using and sharing identifiable Personal Data about Data Subjects who are patients. They should be applied by Users whenever a transfer of patient identifiable data is being considered.

3.3 The Principles are as follows:

3.3.1 Principle 1: Justify the purpose for using the Personal Data

3.3.2 Principle 2: Only use identifiable Personal Data if absolutely necessary

3.3.3 Principle 3: Use the minimum that is required

3.3.4 Principle 4: Access should be on a strict need to know basis

3.3.5 Principle 5: Everyone must understand their responsibilities

3.3.6 Principle 6: Everyone must understand and comply with the law.

3.3.7 Principle 7: The duty to share Personal data can be as important as the duty to protect patient confidentiality.

Schedule 4: Data Breach Process

4. Guidelines

4.1 Data breaches should be contained and responded to immediately on discovering the breach. A Data Protection Impact Assessment should be undertaken immediately to identify the measures required to contain or limit potential damage and recovery from the incident.

4.2 All data breaches, actual and potential must be reported to the Data Protection Officer, the Chief Information Officer and the Head of Information Security immediately a data breach occurs, is threatened or is suspected.. This can be done by completing the Incident Report Form or telephoning +44(0)23 8059 4684 during office hours and Security 02380592811 x22811 outside office hours.

4.3 Users must not try to manage data breaches themselves. **IF IN DOUBT REPORT.**

4.4 The Data Protection Legislation introduces a duty on the University to report certain types of personal data breach to the Information Commissioner's Office as the Supervisory Authority (ICO). within 72 hours of becoming aware of the breach, where feasible.

4.5 Users must co-operate promptly in relation to gathering information relating to the scope of the incident, including completing the Data Breach Incident Report Form.

4.6 Any discussion of the data breach or circulation of information must be restricted to those directly involved in the investigation.

4.7 Any further action will be determined following the investigation.

4.8 The communication of any data breach which involves personal data must be handled with care and advice will be provided.

4.9 Wider communication of a data breach, including notification to the ICO or other regulatory authorities or research sponsors will be managed by the Information Security Response team.

4.10 The Information Governance Group will highlight remedial action which is required in relation to procedures, IT systems, or the data breach reporting procedure. Target data for actions will be logged and followed up by the Information Governance Group.

Schedule 5: Data Subject's Rights

5. Rights

5.1 The Data Protection Legislation enshrines the rights for Data subjects including the rights to:

5.1.1 Request access to data;

5.1.2 Prevent the processing of data for direct-marketing purposes (including profiling) and in certain other circumstances;

5.1.3 Ask to have inaccurate data amended;

5.1.4 Request a restriction to the processing of data in certain circumstances, including to stop processing data where the data subject believes it is likely to cause unwarranted substantial damage or distress to the data subject or someone else;

5.1.5 Request reconsideration of any solely automated decisions made that significant affects the data subject (where such decision-making is legally permissible);

5.1.6 Request that data is provided in a portable (structured, commonly used and machine-readable) format in certain circumstances.

5.1.7 Request the erasure of data.