UNIVERSITY OF Southampton

Data Sharing Protocol

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**.

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

2.3 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).

2.4 This protocol has been designed to provide guidance on the sharing of **Personal** and **Special Category Data** (together known as "Data") to ensure that the University is compliant with the **Data Protection Legislation** as well as its own policies and procedures.

2.5 It should be used as guidance until either a formal Data Sharing or Processing Agreement is in place or until one is agreed. It is not itself a Data Sharing or Processing Agreement as individual projects, initiatives, pieces of work or research should have a bespoke agreement drawn up between all the relevant parties that suit their requirements.

2.6 The definition of Personal Data, Special Category Data and other terms used in this policy are set out in **Schedule 1**.

3 Aims

3.1 The aim of this document is to define how the University should share Data both internally and externally with third parties.

3.2 It will ensure the secure and legal management and processing of any Data shared internally within the University and externally between the University and its stakeholders, collaborators and partners ("third party").

4 Scope

4.1 This Protocol applies to University of Southampton employees, students, agency staff, visitors, contractors and third parties (Users).

4.2 This Protocol applies to agreements that do not include a requirement for the sharing of research data/ data for academic research purposes. If your agreement has a requirement for the sharing of research data / data for academic research purposes, please contact the RIS Research Contracts Team at: **riscontracts@soton.ac.uk** .

4.3 For the purpose of this protocol the types of Data in scope are: Personal Data, Special Category Data, and Anonymised, Pseudonymised and Aggregated Data. See **Schedule 2**.

4.4 Data sharing may include a one off "ad hoc" sharing of Data or a more systematic sharing over a period of time. It can take the form of:

4.4.1 A reciprocal exchange of Data;

4.4.2 One or more organisations providing Data to a third party or parties;

4.4.3 Several organisations pooling information and making it available to each other;

4.4.4 Several organisations pooling information and making it available to a third party or parties;

4.4.5 Exceptional, one-off disclosures of Data in unexpected or emergency situations; or

4.4.6 Different parts of the same organisation making Data available to each other.

5 Principles of Sharing Data

5.1 The continued security of any shared Data will be of the utmost importance.

5.2 Data will not be passed to external third parties or shared internally unless there is a legal and legitimate reason for access and a requirement for the Data in order to carry out that party's function.

5.3 Third parties wishing to have access to Data must either offer a suitable agreement, which the University is willing to sign up to, or sign a University Data Sharing Agreement before any Data is released.

5.4 Where there is an internal request to share Data that has been collected for one purpose with the intention by the internal recipient to use that Data for a different purpose a Data Sharing Agreement must be signed before the Data is released.

5.5 The parties must establish what the Data is to be used for and must agree that it can be used for the purpose defined in any agreement before releasing it.

5.6 An agreed format for the Data must be stated. The format will depend on what the Data consists of, but, where possible, it should be a recognised standard.

5.7 Anonymised, Pseudonymised or Aggregated Data will be used, wherever possible.

5.8 Consideration must be given to the accuracy and the quality of the Data and any Anonymised, Pseudonymised or Aggregated Data to be shared. The parties must ensure that appropriate processes are in place for ensuring that each party holding inaccurate Data corrects it. See the University's Data Quality Policy.

5.9 All Data stored, processed and/or passing through the University must be tracked and recorded to provide an audit trail of where Data has come from and where it is going.

5.10 All Data should be treated with the utmost confidentiality and will only be shared internally or externally by the University if a professional or legal requirement for having access can be demonstrated.

5.11 No Data can be used outside of the University for commercial gain or advantage without the prior agreement of the University.

5.12 Third parties must be able to provide robust audit trails for all Data they hold.

5.13 Every agreement must state the retention periods and deletion arrangements in respect of the shared Data and be regularly reviewed to ensure that the Data sharing is still needed and that its terms are still fit for purpose.

5.14 All staff working with the shared Data must have appropriate Data protection training.

6 Factors to Consider before Entering Agreements

6.1 When deciding whether to enter into an arrangement to share Data consideration must be given to the potential benefits and risks, either to individuals or to society, of sharing the Data. A list of considerations are set out in Schedule 3.

7 Data Sharing & Processing Agreements

7.1 A Third Party may draw up an agreement and the University may only need to sign up to this or agree it is fit for purpose. Where the University is drafting the agreement, please contact Legal Services.

7.2 The purpose of the agreement must be clearly stated and be as simple as possible without being too open or overly restrictive as these form the boundaries within which the shared Data can be used. All parties should agree before any agreement is signed. If a party wishes to change the usage defined in the Agreement then a new agreement should be entered into.

7.3 Each party must be clearly identified and, where possible, their roles or parts they play within the protocol, the names of individuals, their section or department and their addresses must be stated.

7.4 There may be a need to state who owns the Data if it is to be amalgamated with any other Data.

7.5 Should changes be made to the Agreement, each party affected will be informed of the changes and be given time to comment before any changes take effect. If necessary a new agreement should be drawn up.

7.6 Any signed Agreement should be logged with Legal Services.

7.7 Periodic independent audits of third party recipients of Data will take place to ensure that the requirements of the Agreement are being adhered to.

8 Security of Data shared

8.1 The security of the shared Data is of the utmost importance. Measures should be taken to reduce the risk of any security issues arising.

8.2 All Data that is held by the University should be on secure servers or in secure locations, with access restricted to internal use by selected members of staff.

8.3 Each party will have differing security needs, however, it is important that all reasonable steps are made to ensure Data is kept private and confidential at all times. In particular, all parties must take appropriate technical and organisational measures against unauthorised or unlawful processing of Data and against accidental loss, destruction or damage to Data. This will include:

8.3.1 Appropriate technological security measures, having regard to the state of technology available and the cost of implementing such technology, and the nature of the Data being protected.

8.3.2 Secure physical storage, and where possible limitation in the use of portable storage devices or media.

8.3.3 Password protected computer systems.

8.3.4 Restricted access to Data and taking reasonable steps to ensure the reliability of staff who have access to Data.

8.3.5 Appropriate security on external routes into the organisation, for example, internet firewalls and secure dial-in facilities.

8.4 Each party is responsible for complying with privacy legislation, irrespective of the specific terms of stated with any agreement or protocol. Any agreements must be in alignment with the University's Data Protection Policy.

8.5 Each party should give consideration as to how the Data is to be exchanged. This should be assessed against any potential security risks, current policies or legislative requirements. For example, Data should only be sent to an individual as set out in the agreement.

9 Roles and Responsibilities

9.1 The University's Data Protection Officer will oversee the implementation of Data Sharing and Processing Agreements and be responsible for signing off the Data Sharing Agreements that the University enter into.

9.2 All Users who are processing Personal Data are expected to read this Protocol and to understand and apply the principles of the Data Protection Legislation set out in Schedule 4.

9.3 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.

10 Sharing outside EU

10.1 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.

10.2 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 Protocol.

10.3 Where consideration is being given to sharing Data outside the EEA please contact **Legal Services** for advice.

11 Monitoring compliance and review

11.1 This protocol will be subject to periodic audit and review to ensure it remains fit for purpose and the University remain compliant.

12 Further information

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

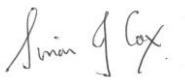
Document Control

File Name	Data sharing Protocol
Original Author(s)	
Current Revision Author(s)	FTVB
Owner	
Publication Date	
Target Audience	

Version History

Version	Date	Author(s)	Notes on Revisions
V1	May 2018		

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 Definitions

1 The following definitions apply to this protocol:

1.1 **Aggregation**: is a data processing technique applied to personal data to produce a generalised result from which individuals cannot be re-identified directly or indirectly ('non-personal data').

1.2 **Anonymisation**:(as defined under the gdpr) is a data processing technique applied to personal data in respect of which a person is non-identifiable taking account of all the means reasonably likely to be used, such as singling out, to identify the natural person directly or indirectly ('non-personal data').

1.3 **Anonymous Data**: information relating to a person rendered such that there is zero risk that can be re-identified or re-identifiable from it (non-personal data).

1.4 **Data Protection Legislation**: (a) any law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding restriction (as amended, consolidated or re-enacted from time to time) which relates to the protection of individuals with regards to the Processing of Personal Data to which a Party is subject, including the Data Protection Act 1998 ("DPA") and EC Directive 95/46/EC (the "DP Directive") (up to and including 24 May 2018) and on and from 25 May 2018, the GDPR and all legislation enacted in the UK in respect of the protection of personal data; and (b) any code of practice or guidance published by the ICO (or equivalent regulatory body) from time to time;

1.5 **Data Processing Agreement**: the Data is being shared with a data processer (an organisation or company processing the Data on behalf of the University as data controller), for example, where the University contracts a specialist marketing company to collate student data for marketing purposes.

1.6 **Data Sharing Agreement**: the sharing of Data between data controllers (where both the University and the third party determine the purposes for which and the manner in which the Data is processed).

1.7 **Personal Data** (as defined under the GDPR): any information that can identify an individual either on its own or in combination with other information and can include photographs and video footage collected and recorded by Surveillance Systems.

1.8 **Pseudonymisation** (as defined under the GDPR): the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

1.9 **Special Category Data**: Personal Data consisting of information relating to the data subject with regard to racial or ethnic origin, political opinions, religious beliefs or beliefs of a similar nature, physical or mental health or condition, sexual life, the commission/alleged

commission of an offence alleged/committed by the data subject and any related court proceedings, trade union membership. It also includes genetic and biometric data where processed to uniquely identify an individual.

Schedule 2 Types of Information

For the purpose of this Protocol, there are essentially three types of data.

1 Personal Data

1.1 **Personal data is data,** which relates to a living individual who can be identified from the data, either on its own or in combination with other information. It also includes expressions of opinion about the individual and any indication of the intentions of the data controller or any person in respect of that individual.

1.2 Note: even things we do not traditionally consider to be personal information such as staff/student identification numbers or online identifiers e.g. cookies are as they can be used to identify the individual.

1.3 Such personal data might include, but not be limited to:

1.3.1 Name

1.3.2 Address

1.3.3 Telephone Number

1.3.4 Age

1.3.5 A unique reference number if that number can be linked to other

1.3.6 Information which identifies the data subject, such as a National Insurance number or Payroll number.

1.4 The law imposes obligations and restrictions on the way the University and its partners process Data. The Data Protection Legislation regards 'processing' of Data to include collecting, storing, amending and disclosing Data. The individual who is the subject of the Data (the 'data subject') has the right to know who holds their Data and how such Data will be processed, including how such Data is to be or has been shared.

2 Special Category Data

2.1 Special Category Data consists of information about racial or ethnic origin, political opinions, religious beliefs or beliefs of a similar nature, physical or mental health or condition, sexual life, trade union membership. It also includes genetic (i.e. inherited or acquired genetic characteristics e.g. blood type) and biometric data (e.g. fingerprints or photographs) where processed to uniquely identify an individual.

2.2 Data concerning criminal convictions or any proceedings is not Special Category Data but is treated in a similar manner.

2.3 Usually restrictions that are more stringent will apply to the use of Special Category Data and any sharing or release will require authorisation by the Data Protection Officer.

3 Anonymised, Pseudonymisation and Aggregated Data

3.1 The processing of non-personal data is not subject to Data Protection Legislation and may not require a data sharing agreement to govern its transfer.

3.2 However, caution needs to be taken when handling Data that has been subject to Aggregation techniques, as it may remain Personal Data. Such aggregations could lead to an individual remaining identifiable e.g. from data sets with small distribution leading to isolation of individual characteristics ('outliers') from which an individual may be singled out.

3.3 Caution also needs to be taken when handling Personal Data that has been subject to Pseudonymisation techniques, as it may remain Personal Data. According to the GDPR, Personal Data, which have undergone Pseudonymisation, which could be attributed to a natural person by the use of additional information, should be considered to be information on an identifiable natural person. Notwithstanding, whether such data could be transformed subsequently into non-personal data depends on whether the risk of identifying the individual has been minimised sufficiently using other techniques such that the person becomes non-identifiable taking account of all the means reasonably likely to be used to identify them.

3.4 As there is a risk that data relating to persons that has been subject to Pseudonymisation (and Aggregation where the data set size is small with unique characteristics) may yet remain personal data, you may still wish to consider putting in place a data sharing agreement to mitigate the risk of a breach of Data Protection Legislation at a later date.

Schedule 3 Factors to Consider

Before entering into a Data Sharing or Processing Agreement you should assess the likely results of not sharing the Data. Ask yourself:

1. What is the sharing meant to achieve? You should have a clear objective/set of objectives. Being clear about this will allow you to work out what Data you need to share and who with.
2. What information needs to be shared? You should not share all the Data you hold about someone if only certain Data items are needed to achieve your objectives e.g. you might need to share somebody's current name and address but not other information.
3. Who requires access to the shared Data? You should employ 'need to know' principles, meaning that other organisations should only have access to your Data if they need it, and that only relevant staff within those organisations should have access to the Data. This should also address any necessary restrictions on onward sharing of Data with third parties.
4. When should it be shared? Document whether the sharing should be an on-going, routine process or whether it should only take place in response to particular events.
5. How should it be shared? This involves addressing the security surrounding the transmission or accessing of the Data and establishing common rules for its security.
6. How can we check the sharing is achieving its objectives? You will need to judge whether it is still appropriate and confirm.
7. What risk does the Data sharing pose? E.g. is any individual likely to be damaged by it? Is any individual likely to object? Might it undermine individuals' trust in the organisations that keep records about them?
8. Could the objective be achieved without sharing the Data?
9. Could the objective be achieved by pseudonymising or anonymising it?
10. Will any of the Data be transferred outside of the European Economic Area (EEA)?

Legal Services will be able to assist in giving you advice and drafting the appropriate agreement for your project.

Schedule 4 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**).