MANCHESTER 1824
The University of Manchester

Standard Operating Procedure

Title:	**Data Protection by Design and Default Standard Operating Procedure**		
Version:	**1.2**	**Effective Date**	**August 2020**
Summary:	Describes the 5 step procedure for applying data protection law, Data Protection Impact Assessment and data protection by design and default principles		

When using this document please ensure that the version you are using is the most up to date by checking on the University's online document system http://documents.manchester.ac.uk/list.aspx for any new versions.

1 Background and purpose

This Standard Operating Procedure ("Procedure") is designed to set out the key stages of implementing Data Protection by Design and Default in respect of all University activities which involve the processing of personal data and thus support the implementation of the Data Protection Policy.

Adherence to this Procedure provides evidence that an appropriate risk assessment of Data Protection compliance and security certification has been undertaken, and ensures that consideration has been given to the data protection implications of any project or activity and the application of all relevant data protection principles before personal data processing takes place, in order to:

- minimise the University's exposure to security, compliance and/or branding and marketing issues, including potential subsequent financial loss, reputation damage or legal exposure;
- clarify the roles and responsibilities of those involved in designing, re-engineering or approving new University processes, physical infrastructure, IT systems, software and/or services or high risk changes;
- identify in a timely manner the individuals, groups, committees or bodies who can advise on the implications of specific data protection law and its application to University processes, physical infrastructure, IT systems, software and/or services;
- identify in a timely manner, relevant parties who may need to sign up to risks and controls specified as part of any commissioned or re-engineered University processes, physical infrastructure, IT systems, software and/or services;
- ensure appropriate procedures are followed before any University processes, infrastructure, IT system, software and/or service becomes live including production or identification of privacy notices; and
- ensure that the on-going support for data protection compliance for University processes, physical infrastructure, IT systems, software and/or services is planned and costed in advance of any commissioning.

2 Definitions and scope

Processing personal data – "processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

This Procedure applies to processing of personal data by the University and all aspects of designing appropriate privacy protection into University activities including proposals, new developments and/or significant changes that involve the access, potential access or processing of personal data. High volume personal data is not defined by the ICO for GDPR but the University considers that systems processing the data of more than 300 data subjects, special category data or data classified as Highly Restricted by the University must be treated as "high risk" initiatives. High risk initiatives relate to processing which affects the rights and freedoms of data subjects.

Activities include, for example:

- Projects involving physical infrastructure where personal data may be processed;
- Non-IT Services developed or acquired software and/or cloud services;
- New IT Services developed or acquired systems, software and/or services and/or;
- Changes to existing IT systems, software and/or services;
- Policy change.

It is not permitted to procure software and/or services which will process personal data without adherence to this Procedure.

3 Procedure and responsibilities

3.1 Consequence of non-compliance with this Procedure

Compliance with this Procedure is mandatory for staff involved in purchasing or designing new physical infrastructure, or updated systems or processes which require the processing of personal data. Non-compliance must be reported to the Head of Information Governance who will determine the action to be taken.

Staff must note that any breach of this Procedure may be treated as misconduct under the University's relevant disciplinary procedures and could lead to disciplinary action. Serious breaches of this Procedure may constitute gross misconduct and lead to summary dismissal.

Any initiative which goes live without following this procedure will be considered to be an information security incident and reported to the Information Governance Committee.

3.2 Responsibilities and key stakeholders

3.2.1 Anyone considering commissioning or changing personal data processing systems must complete the Information Governance Screening Assessment as part of the Information Governance Risk Review ("IGRR") process during discovery or feasibility stages of a project. A decision to introduce a new or updated University system that processes personal data must not be made without completing the IGRR process and completing the 5 steps of the Procedure.

3.2.2 Projects and change initiatives must have a nominated business owner or project manager who is responsible for ensuring that this Procedure is followed. The business owner or project manager must:

- assign an agreed information security classification to the proposed University process, IT system, software and/or service;
- submit and receive approval from the Information Governance Office for their personal data processing activity and entry in the Information Asset Register;
- obtain the required sign-off from the key stakeholders; and

- ensure that the data protection principles listed below are met.

3.2.3 The Information Governance Office and IT Security team are responsible for:

- assessing the risk of submitted proposals, including policy and process changes, and Non-IT Services activities;
- recommending appropriate actions to mitigate risk; and
- approving processing once the required actions have been completed.

Where the residual risk is still considered to be "high risk", the Information Governance Office must consult the Information Commissioner's Office ("ICO") before processing can go ahead.

3.2.4 The Project and Building Data Security Working Group will ensure that Data Protection by Design and Default is implemented in physical infrastructure projects.

3.2.5 The Architecture and Design Review Board, owned by the Head of IT Strategy, Demand and Architecture in IT Services, is responsible for ensuring that Data Protection by Design and Default is embedded within IT-related activities.

3.2.6 The Research Data Management Plans and Research Ethics processes assess research studies and ensure that Data Protection by Design and Default has been implemented.

3.3 The five step IGRR process

Step 1: The business owner or project manager must complete the Information Governance Screening Assessment form on OneTrust as part of the IGRR process early in the life of a project for information processed in any format (e.g. paper, digital) in order to identify the need for a Data Protection Impact Assessment ("DPIA") to be completed in accordance with ICO guidance. The IGRR process is also used to provide a risk assessment of the potential information security impact of all initiatives, not just those which process personal data.

Step 2: The completed OneTrust Screening Assessment form is then reviewed by a member of the Information Governance Office ("IGO"). Where processing is considered "high risk" the business owner or project manager will be asked to provide further information regarding the data being processed and/or the software or store proposed to be used.

Step 3: The business owner or project manager should complete any additional OneTrust assessments to the best of their ability. The technical assessments may require support from IT Services or from the software supplier. Completing these assessments should help to minimise risks and assess whether or not remaining risks are justified rather than eradicating risks.

Step 4: The IGO and, where necessary, IT Security will review these assessments. Completing the assessments is not a one-off exercise and it should be seen as an on-going process as these will form part of the University's Information Asset Register, and must be regularly reviewed with the Information Governance Office. The review period will depend on the level of risk of the initiative.

Step 5: Based on the responses, all "high risk" systems which contain personal data must be designed with evidence of Data Protection by Design and Default being applied, implemented and maintained, and may be audited by the IGO. The questions in the assessments which relate to IT systems and/or services, elicit information which enables IT Services staff to assess compliance with the University's "Data Protection by design" ITS architectural principle which refers to the GDPR definition of "Data Protection by Design and Default". Compliance with this principle involves "taking into account the state of the art [technology], the cost of implementation, and the nature, scope, context and purposes of processing" and the requirement to "implement appropriate technical and organisational measures, which are designed to implement data protection principles (see 3.4) in an effective manner and to integrate the necessary safeguards into the processing."

The completion of the IGRR process and evidence of implementing Data Protection by Design and Default, are required to demonstrate that a DPIA for processing that is likely to be high risk has been carried out. However the approach can also bring broader compliance, financial and reputational benefits, helping the University demonstrate accountability and building trust and engagement with individuals.

3.4 Data Protection Principles

All staff MUST apply the following principles in the planning and development process for personal data in any format:

3.4.1 Lawfulness, fairness and transparency – it must ensure that the project has or develops lawful purpose(s) for the processing and publishes a central and/or local privacy notice approved by the Data Protection Officer or nominated deputy.

3.4.2 Purpose limitation – setting out what appropriate technical and organisational measures have been employed to support the collection of personal data for specified, explicit and legitimate purposes.

3.4.3 Data Minimisation – setting out what appropriate technical and organisational measures have been employed / proposed to ensure personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

3.4.4 Accuracy - setting out appropriate technical and organisational measures to ensure that personal data are kept up to date, taking every reasonable step to ensure data that are inaccurate, having regard for the purposes for which they are processed, and are erased or rectified without delay.

3.4.5 Storage limitation - personal data should be kept in a form which permits identification for no longer than is necessary for the purposes for which it is processed.

3.4.6 Integrity and confidentiality - protecting against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures.

3.4.7 Accountability - the University is responsible for, and must be able to demonstrate compliance with all of the above principles.

4 <u>Monitoring compliance with the Procedure</u>

Heads of School, Directors or equivalent are responsible for ensuring that all staff within their area act in accordance with this Procedure.

4.2 Audit

Evidence of the effective application of Data Protection by Design and Default will be audited periodically.

4.3 Reporting

The Head of Information Governance will report on this Procedure to the Information Governance Committee.

5 Review of Procedure

This Procedure will be reviewed at least every two years or when significant changes are required.

6 Contact list for queries related to this procedure

Role	Name	Telephone	Email
Head of Information Governance	Tony Brown	0161 306 2106	Tony.brown@manchester.ac.uk
Head of Data Protection (DPO)	Alex Daybank	0161 306 2473	Alex.daybank@manchester.ac.uk
Deputy Head of Information Governance	Barbara Frost	0161 275 2122	Barbara.frost@manchester.ac.uk

Version control

Version	Date	Reason for change
1.0	22 May 2018	Initial draft
1.1	30 June 2018	Insertion of disciplinary procedure
1.2	29 July 2020	Updated to include use of OneTrust; reference to audit by IGO

Document control box	
Procedure title:	**Data Protection by Design and Default Standard Operating Procedure**
Date approved:	August 2020
Approver:	Information Governance Committee
Version:	1.2
Supersedes:	1.1
Previous review dates:	
Next review date:	August 2022
Related Statutes, Ordinances, General Regulations:	• Ordinance XIV Intellectual Property Rights (IPR), Data Protection and the Use of Information Systems • University General Regulation XV Use of Information System
Related policies:	• Information Security Policy http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=6525 • Data Protection Policy http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=14914
Related procedures:	• Information classification, ownership and secure information handling: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=29971 • Contracts Governance Policy: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=7926 • Technical Security Standards: http://www.itservices.manchester.ac.uk/aboutus/policy/
Related information:	• Information Governance Risk Review Process (IGRR): • https://www.staffnet.manchester.ac.uk/igo/records-information-management/the-igrr/
Procedure owner:	Head of Information Governance