Standard Operating Procedure

Title: Data Protection governance and responsibilities

Version: 1.0

Effective Date: July 2013

Summary: Description of the responsibilities involved in providing a framework for data protection compliance

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

1 Background

The University has established a Data Protection Compliance Framework, to monitor compliance with the Data Protection Policy and associated Standard Operating Procedures (SOPs), and to provide assurance that the University is maintaining the highest standards in processing personal data.

2 Purpose

The purpose of this SOP is to specify the governance framework and responsibilities which support the implementation of the University’s Data Protection Policy.

3 Reporting and accountability structure

3.1 Board of Governors – Registrar, Secretary and Chief Operating Officer

The Board of Governors has oversight of the broader University policy framework and authorises the Registrar, Secretary and Chief Operating Officer (RSCOO) to issue and review policy statements and procedures to support Statutes, Ordinances and Regulations with which Members of the University must comply.

3.2 Planning and Resources Committee

The Planning and Resources Committee is the University’s principal management committee. It will endorse any policies that are to be forwarded to the Board or its subcommittees for approval. Gaps in policy might be identified within the Board’s subcommittees, or through the University’s Risk and Emergency Management Group.

3.3 Information Governance Committee¹

The RSCOO receives assistance from the Information Governance Committee in carrying out these responsibilities which, in relation to data protection, includes:

- approving plans, procedures, guidance documents and support material produced to assist staff and other approved users in discharging their data protection responsibilities;
- receiving regular reports on data protection issues such as incidents and significant risks; and
- receiving reports on data protection auditing and monitoring throughout the University.

¹ The Data Protection Compliance Group is currently the steering group for establishing a data protection governance framework. It is intended that this group will be replaced by the Information Governance Committee which will be a sub-committee of PRC.
3.4 The **Associate Vice-President (Compliance, Risk & Research Integrity)** provides regular reports from the Information Governance Committee to Planning and Resources Committee and other Board Committees.

3.5 The **Senior Leadership Team** will be consulted on significant matters relating to policies and procedures and are responsible for promoting adoption within their respective areas of operation.

3.6 **All Deans, Heads of School and Directors** are responsible for ensuring that personal data within their areas is processed in line with the Data Protection Policy and established procedures, and for compliance by their staff including:
   - nominating Data Protection Guardians to assist in providing assurance that the Policy and associated procedures are implemented;
   - nominating an Academic Champion to support Data Protection Guardians in academic areas;
   - managing the risks to data protection compliance within their area and ensuring that proportionate arrangements are in place to manage risk; and
   - encouraging all managers and student supervisors to lead by example.

3.7 The **Data Protection Officer** is the nominated officer in the Data Protection register maintained by the Information Commissioner. Supported by the Records Manager, s/he is responsible for overseeing compliance with the Data Protection Policy and associated policies and procedures which describe the measures taken by the University to comply with the Data Protection Act. Responsibilities include:
   - co-ordinating and promoting the University’s Data Protection activities throughout the University;
   - establishing a reporting and accountability structure which includes a network of Data Protection Guardians, providing them with appropriate training and guidance in order to discharge their responsibilities;
   - receiving compliance reports from Data Protection Guardians as outputs from the Self-assessment Toolkit;
   - assisting with the investigation of data protection incidents;
   - providing comprehensive reports to the Associate Vice-President (Compliance, Risk & Research Integrity) on the University’s compliance with the Data Protection Act and related provisions; and
   - liaising with the Records Manager, Information Security Manager, and IT Services to develop and implement awareness and training programmes for the University.

3.8 The primary role of the **Data Protection Guardians (DPG)** is to provide assurance to the Dean, Head of School or Director regarding local compliance with the Data Protection Policy and associated procedures. The DPG is also accountable to the University’s Data Protection Officer. The DPG will normally be a senior member of the Professional Support Services and in academic areas will be supported by a senior academic who will act as an Academic Champion, where appropriate, for matters relating to issues of data protection and information security. DPG responsibilities include:
   - Ensuring that all staff working with personal data are aware of their data protection responsibilities and receive appropriate guidance and training relevant to their job role, maintaining records as evidence;
   - Providing a local point of contact for data protection issues, raising data protection and information security issues at relevant local meetings and escalating actions through the line management structure;
• Disseminating advice and guidance from the Data Protection Officer, Records Management Office and Information Security Manager;
• Maintaining relevant records to evidence effective implementation of procedures at a local level, such as those required for self-assessment and risk assessment procedures, providing reports to the Data Protection Officer and Head of School/Director/Dean as required;
• Performing relevant audits of practice and survey of activity;
• Ensuring that any data protection or information security incidents are correctly notified centrally, and swiftly addressed locally;
• Approving any new data sets or processes which involve the use of staff or student personal data, ensuring that they are in line with the Data Protection Policy and SOPs;
• Identifying circumstances where data sharing or transfer agreements are needed with third parties, and ensuring that these are put in place;
• Ensuring that relevant record storage facilities are fit for purpose; and
• Attending meetings with the University's DPO, including mandatory meetings twice each year.

3.9 **Academic Champion for Data Protection** provides support to the DPG for matters relating to issues of data protection and information security, including engagement and promotion of best practice with the academic community.

3.10 The **Records Management Office** is responsible for:
- Providing expert advice, policies, procedures, guidance and advice in support of the Data Protection Policy and for training staff where necessary;
- Working with DPGs to ensure that documented information is available for provision to students, staff, research participants and others who provide personal data to the University;
- Developing and maintaining processes for data subjects to exercise their access rights in accordance with the Data Protection Act; and
- Undertaking detailed investigation of data protection incidents and, taking advice from the University's General Counsel, determining actions required, liaising with the Information Commissioner’s Office where necessary.

3.11 The **Information Security Manager** is responsible for:
- ensuring that expert advice, guidance and training is available to help keep personal data secure;
- co-ordinating activities where necessary, during the investigation of a data breach;
- maintaining a log of data protection incidents and monitoring that any agreed actions have been completed by the due date, liaising with the Data Protection Guardian to ensure that local actions are promptly completed; and
- updating information security guidance material to reflect any learning outcomes.

3.12 **Information Owners**, including the authors of research papers, dissertations, databases or spreadsheets as well as the managers of core University systems, play a key data protection role. They must ensure that the University policies and procedures are properly applied from inception (ie before any personal data is obtained) until the data is no longer held by the University. They may be required to implement more stringent controls by third-party data providers or external funding bodies.

Where it is necessary to delegate the processing of personal data (eg using third-parties or by enabling access to personal data for the production of reports or data extracts), the Information Owner must establish an appropriate monitoring regime to obtain assurance and evidence that responsibilities are understood and that the controls are operating as required.
3.13 All staff and other approved users of University held personal data must:
- be able to demonstrate competence in their understanding of data protection laws and good practice applicable to the performance of their University responsibilities, as described in the policies, procedures and guidelines established to protect personal data, and must seek advice and guidance if clarification is required; and
- report any actual or suspected data protection incidents, “near misses” or working practices which jeopardise the University’s compliance with data protection legislation.

3.14 The Office of the General Counsel provide legal guidance in relation to data protection matters.

3.15 IT services:
- Undertake damage limitation for IT related data protection incidents eg removing access to files or web pages or suspending central accounts on request from authorized staff;
- Provide appropriate security controls and advice; and
- Determine why the recommended security controls failed in the event of a data breach.

4 Monitoring compliance and effectiveness

The successful implementation of this framework is measured by:
- Review of local self-assessment documentation;
- Annual Compliance Exercise;
- Feedback from staff;
- Analysis of the responses and audits of collaborating organisations;
- Review of the severity and frequency of data protection incidents and near-misses; and
- Risk-based programme of audits of staff and systems.

5.0 Contact list for queries related to this procedure

<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
<th>Telephone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deputy Secretary/Data Protection Officer</td>
<td>Martin Conway</td>
<td>0161 306 3772</td>
<td><a href="mailto:martin.conway@manchester.ac.uk">martin.conway@manchester.ac.uk</a></td>
</tr>
<tr>
<td>Records Manager</td>
<td>Alan Carter</td>
<td>0161 275 8111</td>
<td><a href="mailto:alan.carter@manchester.ac.uk">alan.carter@manchester.ac.uk</a></td>
</tr>
<tr>
<td><strong>Document control box</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Policy / Procedure title:</strong></td>
<td>Standard Operating Procedure – DP reporting and accountability structure</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Version:</strong></td>
<td>1.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Date approved:</strong></td>
<td>July 2013</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Approved by:</strong></td>
<td>Data Protection Officer (Martin Conway)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Supersedes:</strong></td>
<td>Version 1.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Next review date:</strong></td>
<td>July 2015</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Related policies and procedures:</strong></td>
<td>See <a href="http://www.dataprotection.manchester.ac.uk/policiesandprocedures/">http://www.dataprotection.manchester.ac.uk/policiesandprocedures/</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Related guidance and or codes of practice:</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Related information:</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Policy owner:</strong></td>
<td>Data Protection Officer (Martin Conway)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Lead contact:</strong></td>
<td>Data Protection Officer (Martin Conway)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>