1 Background

The Data Protection Act 1998 regulates the way in which organisations collect, hold, use and dispose of personal data. These activities are collectively known as “processing”. The Act lists 8 principles which organisations must apply when they are processing the personal data of individuals.

The fifth data protection principle states that “personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes”

Personal data which is kept for longer than necessary breaches the Data Protection Act and puts the university at risk of regulatory action from the Information Commissioner’s Office.

Personal data remains at risk of a data breach whilst it exists, and is also disclosable under data protection and freedom of information legislation. Keeping old data clutters systems and makes active data harder to find.

Disposing of data in line with clearly defined policies reduces the risks of destroying valuable current data by accident, as can happen when data is destroyed due to lack of space or an unplanned clear-out.

For all of these reasons it is important that all personal data held and used by the University has a retention policy attached to it, and that these policies are adhered to.

2 Purpose

This standard operating procedure (SOP) applies to the processing of all personal data by The University of Manchester.

The purpose of this SOP is to define those procedures which apply to the retention of personal data by the University of Manchester to ensure that it is only kept for as long as is necessary.

3 Procedures

3.1 Purpose for obtaining data

When the University collects and processes personal data it must do so for specified purposes. The data subjects concerned must be informed of these purposes through a fair collection notice. The purposes for which the University is registered to process personal data are listed here:
After personal data has been collected, and whilst it is held and used by the university, it must only be used for the purpose(s) for which it was collected, and must have policies assigned to it which reflect this purpose. One of these policies should be a retention policy.

### 3.2 Retention policies

A retention policy defines how long a piece of data should be retained for, and what should happen to it once that retention period has been fulfilled. It is not always the case that a piece of data should be destroyed once it reaches the end of its retention period. Some data for example is passed to the University archives for permanent retention or for review.

The University has a retention schedule which covers the most common types of data held.

It is important that retention policies should be consistent across the University. It is difficult to argue, for example, that one School needs to keep a certain type of data for longer than another School if both sets were collected for the same purpose. If local needs dictate that a record is kept for longer than suggested by the retention schedule please consult with the Records Management Office so that a suitable period can be agreed and added to the University schedule.

Data which needs to be kept for a period of time longer than seven years, and which is not covered by the retention schedule, must have a written justification for this retention agreed by the Records Management Office.

### 3.3 Putting retention policies into practice

It is not always easy to implement retention policies. Often weeding out data which has reached the end of its retention period is a time consuming and labour intensive process. It may also be difficult to remove data from electronic databases.

It is important, however, that retention policies are adhered to for reasons given above. Thought should be given as to how records are to be identified and destroyed when a filing system or database is being designed.

It should always be possible to easily delete data from an electronic database. This should be part of the procurement or design process, and personal data should not be kept within systems from which it is difficult to delete it. Note that masking or “archiving” data does not count as deletion - it must be permanently removed from the system and backups before it can be counted as no longer held by the University.

It can also sometimes be difficult to identify data to be disposed of. A file relating to a single individual may contain data collected and held for different purposes (financial, pastoral, administrative, academic etc). If each of these purposes attracts a different retention policy and period, this can mean that the same file has to be weeded of data at several different times. Conversely, if information is stored by purpose (for example all financial documentation is stored together) it can be difficult to identify all documentation relating to a particular individual. Filing systems, both paper and electronic, should be designed in such a way as to facilitate the application of retention policies relevant to the data contained within them. If for example you need to dispose
of files relating to particular individuals 6 years after they leave the University it is sensible to
arrange files by name within years, and to have some system of tagging files to record leaving date.

Compliance with the Data Protection Act requires that sufficient staff time and resource be provided
to ensure that personal data is disposed of in a timely manner. It is sensible therefore to limit the
resource necessary by ensuring that this data is easily identified and disposed of, and that retention
policies are widely known and understood by staff who work with personal data.

4 In summary

The University must only keep personal data for the length of time necessary for the purpose(s) for
which it was collected.

The University maintains a retention schedule to record the periods for which it will keep personal
data and what will happen to it once that period has been reached. Personal data not covered by the
retention schedule must also have retention policies assigned to it.

Retention policies must be uniform across the university, and deviations from the retention schedule
must be justified.

Filing systems and database designs must reflect the necessity for regular and controlled removal
and deletion of data.

5 Contact 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>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>
</tbody>
</table>

Document control box

<table>
<thead>
<tr>
<th>Procedure title:</th>
<th>Standard Operating Procedure - Data Protection Principle 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version:</td>
<td>1.0</td>
</tr>
<tr>
<td>Date approved:</td>
<td>June 2013</td>
</tr>
<tr>
<td>Approved by:</td>
<td>Martin Conway</td>
</tr>
<tr>
<td>Supersedes:</td>
<td>N/A</td>
</tr>
<tr>
<td>Next review date:</td>
<td>June 2015</td>
</tr>
<tr>
<td>Related policies and procedures:</td>
<td>Data Protection Policy, Data Protection Standard Operating Procedures</td>
</tr>
<tr>
<td>Related guidance and/or codes of practice:</td>
<td>Data Protection Guidance</td>
</tr>
<tr>
<td>Related information:</td>
<td>ICO guidance on Data Protection Principle 5</td>
</tr>
<tr>
<td>Policy owner:</td>
<td>Data Protection Officer (Martin Conway)</td>
</tr>
<tr>
<td>Procedure owner:</td>
<td>Records Manager (Alan Carter)</td>
</tr>
</tbody>
</table>