CONFIDENTIAL DATA

1. Introduction

This policy sets out roles and responsibilities for handling / storing / processing confidential data, and provides links to relevant resources.

2. Definitions and scope

Confidential data are those which classify as either *medium* or *high* risk in the University's Information Risk Classifications. Confidential data may or may not be personal data; however most personal data will be confidential. This policy applies to all confidential data used as part of University work, or stored or processed on University systems. It applies to data in electronic and other formats e.g paper.

3. Roles and Responsibilities

3.1 Information User

Information users must handle the data in accordance with the measures defined by the data owner. If the information owner hasn't yet done this, then the Confidential Data Guidelines are a good start.

3.2 Information Owner

The information owner must:

- Be clear what data are stored/processed.
- Be aware of the consequences if the data were to fall into the wrong hands, and what risks might cause this to come about.
- Define (or at least propose) the mitigation measures that protect the data, reducing these risks to an acceptable level. In many cases, the Confidential Data Guidelines may be appropriate, but this will not always be the case.
- If personal data are involved, it may be necessary to undertake a Data Protection Impact Assessment.
- Record the above in the University Information Asset Register.

3.3 Information Risk Owner

The IRO will ensure the above happens and approve the processing activity. This includes giving consideration to whether:

- the risk assessment is sufficiently thorough
- the measures proposed are appropriate
- the overall risk has been reduced to an appropriate level.

As a part of this, the IRO may consult with Information Security Team and the Data Protection & Freedom of Information Office.