

# CONFIDENTIALITY POLICY

## 1. PURPOSE

The purpose of the policy is to set out expectations for how Cardiff University will handle confidential information.

## 2. SCOPE

This policy applies to staff, students and any other party handling information for which Cardiff University owes a duty of confidence.

## 3. RELATIONSHIP WITH EXISTING POLICIES

This policy forms part of the Information Security Management Framework. It should be read in conjunction with the Information Security Policy.

It also has a relationship with other University policies specifically:

- Data Protection Policy
- Records Management Policy

## 4. POLICY STATEMENT

- 4.1 The University holds confidential information (*See Definitions*) about individuals and other non-personal confidential information, e.g. information about business finances, strategy and planning.
- 4.2 Staff and students are under a common law obligation not to disclose confidential information inappropriately, whether it relates to people or otherwise.
- 4.3 Staff are also contractually obliged to maintain 'mutual trust and confidence' with the University and not to disclose confidential information without proper authorisation.
- 4.4 Students should not normally have access to the University's confidential business records, although it is recognised that they may, legitimately, come into the possession of confidential information through the course of their studies, membership of University committees, etc.
- 4.5 Anyone processing personal confidential information (e.g. transcribers, consultants) on behalf of the University must only do so under contract.
- 4.6 Deliberate or reckless breaches of confidence relating to confidential information held by the University may be treated as a disciplinary offence (under either staff or student disciplinary procedures) and may constitute an offence under Data Protection law. Such breaches may also be actionable by the party whose confidence has been broken and result in litigation against the individual who breached the confidence.
- 4.7 Members of staff performing a supporting role in a professional capacity (e.g. Health Centre medical staff, chaplains and counsellors) will be bound by their professional codes of practice in respect of the maintenance of confidentiality. The NHS (in common with the University) takes the confidentiality of its patient records very seriously and all those having access to medical records, including students, should ensure that no inappropriate disclosures of such information are made.

- 4.8 All staff should ensure that they are familiar with the document '[Confidentiality – A Guide for Staff](#)' available from the Assurance Services, Strategic Planning and Governance.

## 5 RESPONSIBILITIES

All staff and students should ensure that any confidential information concerning University business for which they are responsible is stored securely in line with the [University Information Classification and Handling Rules](#) and in such a way that confidentiality is maintained.

## 6 COMPLIANCE

All alleged breaches of the confidentiality shall be notified to the University IT Service Desk as per the Information Security Incident Management Procedure. Any infringement by staff or students may expose the University and/or the individual to legal action, claims for substantial damages and, in the case of confidential information containing personal data, fines from the Information Commissioner. Any infringement will be treated seriously by the University and may be considered under relevant disciplinary procedures.

## 7 KEY DEFINITIONS

### ***Confidential Information***

Confidential information is defined in categories C1 and C2 of the [University's Information Classification and Handling Guidelines](#) and includes any information to which the common law 'duty of confidence' applies. A duty of confidence is created when 'private' information has been passed on in such a way that the person receiving the information was aware, or should have been aware, that the information was being imparted on the basis of confidentiality. (The legal test is whether a 'reasonable' person would think the recipient ought to have known that the information was confidential).

### ***Personal Data***

Confidential information may include personal data which is any recorded information about a living individual who can be identified from that data or from that data and other available data. This includes, inter alia, information held in paper records, electronic records, digital files, video and audio recordings, photographic images.



**Document Control Table**

<b>Document Title:</b>	Confidentiality Policy
<b>Author(s) (name, job title and Division):</b>	Senior Assurance Advisor, Department of Strategic Planning and Governance
<b>Version Number:</b>	1.2
<b>Document Status:</b>	Approved
<b>Date Approved:</b>	29 June 2015
<b>Approved By:</b>	Information Security Review Group
<b>Effective Date:</b>	May 2018
<b>Date of Next Review:</b>	May 2020
<b>Superseded Version:</b>	1.1

**Document History**

<b>Version</b>	<b>Date</b>	<b>Author</b>	<b>Notes on Revisions</b>
Ver 1.0	November 2012	Ruth Robertson	
Ver 1.1	June 2015	Matt Cooper – Information Rights Manager	Reformatted to template, added sections on responsibilities and compliance. Updated definitions of confidential information
Ver 1.2	May 2018	Matt Cooper – Senior Assurance Advisor	Review and minor updates