CONFIDENTIALITY POLICY

1. Purpose and Scope

The purpose of the policy is to set out expectations for how Cardiff University will handle confidential information. Confidential information is defined as categories C1 and C2 of the University's Information Classification and Handling Policy and includes any information to which the common law 'duty of confidence' applies. Such confidential information can be contained in confidential university business records and can include personal data, as defined in data protection legislation.

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.)

This policy applies to members of Cardiff University as defined under Ordinance 2 – Members of the University and any other party engaged where confidential data is processed on behalf of Cardiff University.

2. Policy

The university holds confidential information about individuals and other non-personal confidential information, for example information about business finances, strategy and planning. Where the university is handling personal information for which a common law 'duty of confidence' applies, the provisions of the Data Protection Policy will also apply.

Staff and students are under a common law obligation not to disclose confidential information inappropriately, whether it relates to people or otherwise.

Staff are also contractually obliged to maintain 'mutual trust and confidence' with the university and not to disclose confidential information without proper authorisation.

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.

Anyone processing confidential and/or personal information (for example transcribers, consultants) on behalf of the university must only do so under an appropriate contract.

Deliberate or reckless breaches of confidence relating to confidential information held by the university may be treated as a disciplinary matter (under either staff or student 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.

Members of staff engaged in providing support to students where there are serious concerns about their health or wellbeing may, on the decision of appropriately senior and/or qualified member of staff, share confidential information with a student's nominated trusted contact and relevant agencies or third-party organisations. Students are asked to provide details of trusted contacts during the enrolment process and are provided with guidance on how we will disclose their personal information to the nominated trusted contact. Any sharing will be in accordance with university guidelines developed in the best interests of supporting students, staff and the community.

Members of staff performing a supporting role in a professional capacity (for example 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.

3. Roles and Responsibilities

All individuals shall:

- 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 Policy and in such a way that confidentiality is maintained;
- ensure that they are familiar with the guidance on confidentiality on the staff intranet;
- ensure that all sharing is in accordance with the relevant internally developed guidelines for specific circumstances;
- not knowingly, or recklessly disclose information in which there is a duty of confidence;
- report any alleged breaches of confidentiality to University IT Support as per the Information Security Incident Management Policy.

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 of this policy will be treated seriously by the university and may be considered under relevant disciplinary procedures.

4. Related Policies and Procedures

This policy forms part of the Information Security 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

Document Name:	**Confidentiality Policy**
UEB Policy sponsor	Senior Information Risk Owner - University Secretary and General Counsel
Policy Owner:	Senior Compliance and Risk Advisor and Data Protection Officer, University Secretary's Office
Policy Author:	Senior Compliance and Risk Advisor and Data Protection Officer, University Secretary's Office
Version Number:	1.3.1
Equality Impact Outcome and Form Submission Date:	July 2022
Approval Date:	November 2023
Approved By:	Senior Information Risk Owner
Date of Implementation:	December 2024
Date for Next Review:	December 2027
For Office Use – keywords for search function	