Guidelines for the use of Turnitin at Curtin
Clarification on arrangements for account security

This document should be read in conjunction with the Guidelines for the use of Turnitin at Curtin, which forms Schedule G of the Plagiarism Policy and Procedures.

Background

Curtin subscribes on an institutional basis to the web based software ‘Turnitin’, used for checking originality in submitted work. Turnitin is hosted on a server in the USA, and at this point in time, it operates as a system independent of the Curtin Blackboard learning environment. Turnitin is in common use world-wide.

Turnitin has a number of strengths, but there are some significant weaknesses in terms of:

1. **Administration** (Curtin Turnitin administrators are unable to see an individual tutors Turnitin class, which has implications for the provision of support by the Assessment Centre.)
2. **Class configuration** (Turnitin limits access to one tutor per class – this poses problems for larger cohorts that are taught by teams of staff.)

Schedule G of the Plagiarism Policy addresses point 1 as follows:

“The Turnitin account system does not permit administrators to directly access an Instructor’s account. To be consistent with Curtin’s Password Security Policy, Assessment Centre staff will not ask a user to reveal their password. To enable access for the purposes of providing support the user will be instructed to temporarily change their password to a specified string of characters. Once the issue is resolved the user will be instructed to change this password so that the security of the system is ensured.”

This document clarifies the University position with respect to the significant issues raised by point 2. Firstly, colleagues are reminded that Schedule G of the Plagiarism Policy and Procedures specifies that:

“Turnitin accounts for Instructors or Teaching Assistants MUST NOT use the same password as the user’s Curtin or OASIS account password. Passwords should not be shared between users, doing so is a breach of Curtin’s Password Security Policy.”

Instructors and Teaching Assistants (tutors) log in to Turnitin using their Curtin email address as their user ID. As indicated in the restriction quoted above this user login must not be shared with other users, doing so is a breach of Curtin’s Password Security Policy.

Turnitin accounts that have been set up using a generic/shared Curtin email account address as the user ID can be shared by members of the teaching team, as authorised by the Unit Coordinator. The shared password must be kept in strictest confidence.

**Shared accounts and the responsibilities of the Unit Coordinator**

Unit Coordinators should ensure that there are clear and defensible procedures in place for managing access to the Turnitin environment. In order to mitigate risks and in compliance with Curtin Information Security Policy, procedures should be established by the Unit Coordinator for the induction of new staff to the shared account. Passwords shall meet the complexity requirements as detailed in the Password Security Standard. Procedures must be established for routine password renewal at the end of the teaching period or when a staff member leaves the teaching team. Users who no longer administer a particular system must have their access rights removed from the system immediately.