Computing Conditions of Use Policy

Section 1 - Definitions

(1) For the purpose of this policy:

a. Account - Secured personal access to facilities in the form of a username and password.
b. Archiving - Older data is moved to an alternate storage location. The primary purpose is to provide a facility to retain older corporate data, while 'freeing space on the central storage area for current work.
c. Backup - A copy of data taken at a particular designated time. The primary purpose is to provide a disaster recovery copy of data in the case of a server or hard disk failure.
d. CD-R - Compact Disc - Recordable
e. Computing and telecommunication facilities - All facilities that are owned, leased and operated by the Technology Services department.
f. Conditions of Use - The conditions, ethics and practices that all computing users at SCU should adhere to in order to comply with the University's policy for acceptable use as detailed in the Computing Conditions of Use policy.
g. Delegated Officer - A member of the university staff appointed in writing by the Executive Director, Corporate Services to deal with breaches under this part.
h. DVD-R - Digital Video Disc - Recordable
i. Email (electronic mail) - An electronically transmitted message, which arrives as a computer file on your PC via the University's server. A University record in the form of electronic mail exists whenever such electronic mail is in support of University business, whether or not the University owns the equipment, software, or facilities used to create, or store the electronic mail record. The terms electronic mail and email are used interchangeably throughout this policy.
j. HTTP - Hyper-text transport protocol
k. IT - Information Technology
l. Netiquette - Etiquette practiced or advocated in electronic communication over a computer network.
m. Network - The University network hardware and the services working on the hardware or utilising the hardware to carry out tasks.
n. Review Officer - The member of the university staff appointed in writing by the Executive Director, Corporate Services to deal with appeals this part.
o. SCU - Southern Cross University
p. SOE - Standard Operating Environment - Baseline software suite supporting core information systems of the University. Includes Operating System, email client, word processing, software spread sheeting, presentation, internet access, and administration system access software.
q. System Administrator - An authorised person that has administrative rights to IT systems.
r. User - Any person who makes use of any IT system, hardware or service from any location. Staff, student and University trainee, associate or partner and bona fide visitor.
s. University - Refers to Southern Cross University.
t. U Drive - Personal service space - accessible only by staff member.
u. W Drive - Shared work space - accessible by all members of a work unit.

Section 2 - Policy Statement

Part A - Policy Declaration

(2) University Computing Services are University facilities intended to support and enhance efficiency in teaching, learning, research and administration activities. The University encourages the use of the University's computing services to enhance communications and to expand the educational and research resources available to staff and students, and also for encouraging internal collaborations within the University itself.

(3) Use of the University's computing and telecommunication facilities is subject to the State and Federal laws that apply to computing and telecommunication as well as other relevant legislation, policy and regulations.

Part B - Policy Description

Objectives

(4) This policy has been developed to:

a. Clarify the responsibilities and ethics related to the acceptable use of the computing and telecommunication facilities at Southern Cross University
b. Encourage appropriate use of the computing and telecommunication facilities at Southern Cross University
c. Inform the University community of the conditions associated with the use of computing and telecommunication facilities
d. Comply with relevant State and Federal legislation, policy and regulations.

Scope

(5) This policy applies to:

a. All computing services provided or owned by the University.
b. All users and uses of University computing services.

(6) Any person using the University's computing facilities or services is bound by this policy.

Part C - Content and Implementation

(7) This Policy addresses details necessary for the overall Computing Conditions of Use Policy to operate effectively throughout the University. It covers the areas of:

a. Access and Availability;
b. Security;
c. Internet & Intranet Conditions of Use;
d. Network Conditions of Use;
e. Computer Workstation Conditions of Use;
f. Remote Access Conditions of Use;
g. Email Conditions of Use;
h. Software Conditions of Use;
i. Web Hosting and Web Publishing Conditions of Use;
j. Management and Monitoring;

k. Training; and
l. Advice and Assistance.

Part D - Access and Availability

(8) The University computer system environment is in place for the users to be able to perform their duties as needed, and therefore users shall respect and be responsible for this environment. It is assumed that a user will use the environment in an ethical and lawful way.

Access to Computer Systems

(9) Access to the University's computing and telecommunication facilities is available to a user for approved teaching, research and administrative purposes. In the case of students this access is only for purposes directly related to their academic programs.

(10) Most computing facilities provided by SCU require user authentication (the use of a username and password). Usernames and password, or what is often referred to as an "account", is automatically created on commencement of employment or admission to the University.

(11) Users shall not use any other person's computer account unless it is a special group account authorised by the Chief Information Officer, an approved nominee or the relevant administrator.

(12) Users shall not allow any other person to use their computer account.

Exclusive Use of a Facility

(13) A user who has an approved booking for a specific facility and who has not abandoned that booking shall have exclusive use of that facility during the booked period.

(14) The University reserves the right to withdraw the availability of any computing and telecommunication facility without notice to ensure the integrity and security of the University network. However, wherever possible, Technology Services will endeavour to notify staff and students prior to withdrawing the service.

(15) A user shall not collect nor discard any electronic, printed data or storage medium which is not their property or the property for which they have authorised access.

(16) Information stored, transmitted or processed by the University's computer and telecommunication facilities must not contain any illicit materials. Users shall under all circumstances ensure that print, language or visual materials are used only for legitimate University purposes.

Commercial or Profit Making Activities

(17) A user may not use the computing or telecommunication facilities for or on behalf of any party for the purpose of profit making or commercial activity, unless written permission has been obtained from the Chief Information Officer or an approved nominee. Advertising or sponsorship is not permitted except where such advertising or sponsorship is clearly related to or supports other services being provided to by Southern Cross University.

Online Feedback and Comment Mechanisms

(18) Similarly to staff and student email discussion forums (see Email Policy), the use of online feedback and comment mechanisms, such as online surveys and questionnaires, is to be in accordance with all laws and acts of Australia, and relevant Southern Cross University statues, rules and policies including, but not limited to:

a. Harassment, Bullying and Discrimination Policy
b. Code of Conduct
c. Watch Your Language: Non Discriminatory Language Guidelines

(19) Online feedback and comment mechanisms are made available for the use of all Southern Cross University staff and students. Language or content that is considered by a reasonable person to be threatening, harassing, defamatory or slanderous, abusive, obscene, fraudulent or discriminatory is in breach of the University's Code of Conduct, relevant policies and statutes, and is not permitted when using online feedback or comment mechanisms.

(20) The law of defamation is complex, and seeks to balance free speech with the right of an individual or organisation to protect their reputation. Users are advised to research the issue of defamation and to ensure that they do not unintentionally post defamatory content when using online feedback and comment mechanisms.

Vandalism

(21) It is a breach to remove, deface or corrupt notices or records which are placed by authorised University staff for the purpose of promulgating policy and rules or assisting in the operation of the computing facilities.

Expressions of Personal Views

(22) A user must be aware that the correspondence and discussion in to which they enter when using the University network and the Internet may be construed to be representative of the University's position.

(23) Where the client does not have authority or is not aware of the University's position or where their personal view may vary from that of the University, such correspondence must clearly state that "the opinion expressed is that of the writer, and not necessarily that of the University", or words to that effect.

Official Representation of the University

(24) Where the user is representing the views of the University, then a notation must be appended to the communication identifying the individual and the position title held within the University.

Harassment of Others

(25) A user shall not use computing and telecommunication facilities for the intent to defame, slander or harass others, or to interfere with their work. It is a breach of this policy to send obscene, abusive, fraudulent, threatening or repetitive messages to a user or users. A user is bound by University policy and guidelines associated with conduct and equity practices and therefore will behave in such a manner that is professional and sound.

Disclaimer

(26) The University accepts no responsibility for any damage to or loss of data, hardware or software arising directly or indirectly from use of the University's computing and telecommunication facilities or for any consequential loss or damage. The University makes no warranty, express or implied regarding the facilities offered, or their fitness for any particular purpose. Additionally, Technology Services staff will not be held liable for any damage to or loss of data, hardware or software whilst carrying out their duties.

Part E - Security

Passwords

(27) Users must, for their own security:

a. Not give their password to anyone else
b. Change their password frequently (e.g. every 90 days)
c. Make it a secure password.

(28) Secure passwords are:

a. More than eight characters long
b. A combination of upper and lower case letters
c. A combination of letters and numbers
d. Not easily identifiable (e.g. do not use your given name).

Resetting Passwords

(29) Users need to change passwords regularly. For further information, please refer to the Password Protection web page.

Rights to Privacy and Security

(30) Users of the University's computing and telecommunication facilities have the right, subject to Part I (Management and Monitoring) of this document and in accordance with the Workplace Surveillance Act 2005 to privacy and security of their computer programs and data.

(31) A user shall not copy, disclose, transfer, examine, rename, change, add to or delete software, data or information belonging to another user without that user's permission.

(32) The University has a number of security policies that the University community should be familiar with.

(33) The University community is responsible for the security and protection of IT information and systems.

(34) The policies are available from the Technology Services home page.

Part F - Internet and Intranet Conditions of Use

(35) All SCU information and communication technology is provided with direct network connection to internet facilities. Access to and use of the internet is for teaching, learning, research and administration purposes.

(36) The following conditions apply to the use of the Internet and Intranet at the University.

(37) A general notification will be provided to users outlining the terms and conditions. Refer to Part I.

(38) For effective management of data download, data traffic will be monitored and specific sites blocked primarily those that violate copyright.

(39) You should not use the University network to access inappropriate internet sites. Inappropriate internet sites include but are not limited to:

a. Gaining unauthorised entry to other sites
b. Pornography
c. Unauthorised streaming video, music, internet radio, online games, file-sharing
d. Gambling/Gaming
e. Violation of copyright
f. Deliberate spreading of viruses or malicious code

g. Recreational Chat.

Part G - Other Conditions of Use

(40) For:

a. Network Conditions of Use - refer Network Policy
b. Computer Workstation Conditions of Use - refer to Computer Workstation Policy
c. Remote Access Conditions of Use - refer to Remote Access Policy
d. Email Conditions of Use - refer to Email Policy
e. Software Conditions of Use - refer to Software Policy
f. Web Hosting and Publishing Conditions of Use - refer to Web Hosting and Publishing Policy

Part H - Copyright Conditions of Use

(41) The University computing and telecommunication facilities must not be used to copy software, upload or download material that is licensed or protected under copyright or trademark laws unless such activities fall within current licensing conditions and/or copyright legislation. Users must abide by copyright legislation and relevant University policy.

(42) Information pertaining to copyright and copyright guidelines can be obtained from the University's Copyright website.

(43) If you believe copyrighted work is available on the Southern Cross University network in such a way that constitutes copyright infringement, or a breach of an agreed licence or contract, a "Takedown Notice" form is available via the Legals link at the bottom of all Southern Cross University website pages.

Part I - Management and Monitoring

(44) Any person using the University's computing facilities or services is bound by the Computing Conditions of Use Policy and all Technology Services policies and their associated procedures. These policies are found on the SCU Policy Library home page.

(45) Terms and conditions for use of the SCU Computers and/or Network will be displayed to users on a monthly basis at the initial log on for each month. Appendix A outlines the terms and conditions.

Workplace Surveillance

(46) Notwithstanding the provisions of Part E, clauses (30) to (34) (Rights to Privacy and Security), in accordance with the Workplace Surveillance Act 2005, the Vice Chancellor and nominee(s) and relevant system administrators have the right to examine all computer files and to monitor computer usage to ensure compliance with these rules and to maintain a secure, efficient computing and telecommunication environment. Technology Services endeavours to provide a secure network and computer systems. Users using the computer systems may have any of their activities on systems monitored and recorded by system administrators.

(47) The University monitors staff and students use of University computers and IT systems in the following areas:

a. University workstations, servers, email and network services, printers, network connected devices and connections to the internet.
b. The University retains logs, backups and archives of computing activities which may be audited. Such records are the property of the University, are subject to State and Federal laws and maybe used as evidence.

c. Monitoring may include but is not limited to: storage volumes, download volumes, copyright, suspected malicious code or viruses.
d. All Technology Services computing facilities are under constant video surveillance.

(48) Users are advised that if such monitoring reveals evidence of misuse, system administrators may act to secure the University system and will provide such evidence to the appropriate authority.

Non-compliance

(49) In accordance with Student Misconduct Rules the Chief Information Officer or nominee may take immediate action to deny any user access to those computing and telecommunication facilities under control of Technology Services, as a consequence of any action which is deemed to be detrimental to computing and telecommunication hardware, software or data and/or in non-compliance with any statute, University policy, procedures or guidelines.

(50) Any action taken by Technology Services staff to suspend access by a user to computing and/or communications facilities shall be reported immediately to the Chief Information Officer or nominee who shall recommend what further action should be taken in accordance with the provisions of the University Rules.

(51) Any action taken by a user that violates any State or Federal legal statute, particularly in relation to abuse of federal telecommunication facilities, copyright, Privacy Act and possession or distribution of specific categories of pornographic material, shall be viewed as a criminal offence and will be referred to the appropriate enforcement authority. This may result in criminal investigations/proceedings being taken against the offender.

Knowledge of Breach of Policy

(52) Should any person become aware of any action by another individual which could be considered to breach this policy, they are requested to take appropriate action to ensure it is brought to the attention of the Technology Services Client Services Manager The report may be provided orally or in writing to the Technology Services Client Services Manager - Email TSfeedback@scu.edu.au or Phone 02 6620 3481.

Part J - Training

(53) It is the responsibility of the teaching staff to familiarise themselves with the IT computing and telecommunication facilities, including lecture theatres and teaching spaces, prior to tutorials or workshops.

(54) Training sessions on familiarisation with labs and equipment are conducted at the start of each semester.

(55) Staff are notified of these sessions via email.

Part K - Advice and Assistance

(56) For further advice or assistance, please contact the relevant SCU Call Centre listed below:

a. Lismore Campus - Email servicedesk@scu.edu.au or Phone: 02 6620 3698
b. Tweed/Gold Coast Campus - Email servicedesk@scu.edu.au or Phone: 02 6620 3698
c. Coffs Harbour Campus - Email coffs.servicedesk@scu.edu.au or Phone: 02 6659 3080

Section 3 - Related Policies, Documents, Legislation

and Strategic

Institutional Context

(57) All staff and students are required to be aware of this policy and on commencement or enrolment to the University they should be provided with a copy or referred to the website.

Section 4 - Responsibilities

Responsibilities and Approvals

(58) The Chief Information Officer is responsible for the periodic review and recommended changes to the Conditions of Use to ensure they remain valid and consistent.

(59) The Chief Information Officer is responsible for ensuring that the Computing Conditions of Use are observed with regard to the services under the control and management of Technology Services.

(60) The Chief Information Officer will recommend to the University Executive appropriate Computing Conditions of Use to meet the legislative and operational needs of the University.

(61) Each Head, Faculty /Head, Department /Head, Centre /Head of School /Head of Work Unit is responsible for providing education and awareness to ensure that all staff and students associated with their area comply with the Computing Conditions of Use.

(62) Users shall not use any other person's computer account unless it is a special group account authorised by the Chief Information Officer, an approved nominee or the relevant administrator.

(63) Users shall not allow any other person to use their computer account.

Section 5 - Procedures

Part L - General Procedures Related to Computing Conditions of Use Policy

Re-setting Passwords

(64) To obtain new passwords the user will need to contact the relevant SCU Call Centre:

a. Lismore Campus - Email servicedesk@scu.edu.au or Phone: 02 6620 3698
b. Tweed/Gold Coast Campus - Email servicedesk@scu.edu.au or Phone: 02 6620 3698
c. Coffs Harbour Campus - Email coffs.servicedesk@scu.edu.au or Phone: 02 6659 3080

Unauthorised Connection of Equipment to the Network

(65) To be able to connect personal equipment to SCU Network, the user will need to fill out a Connection of Personal Equipment to the SCU Network form which is available from:

a. Website - Link to Non-Standard Account Request Form
b. In person - Technology Services Reception, Level 1, A block, Library

(66) The form will need to be completed and signed by the appropriate Director or Head of School /Head, Department /Head, Centre /Head of Work Unit.

(67) The form is sent to Technology Services Reception, Level 1, A block, Library for the Chief Information Officer to approve.

(68) If approved, the form will be logged with the SCU Call Centre and the user will be notified for an appropriate time for the laptop to be configured for the SCU network.

(69) If not approved, the user will be notified as soon as practicable.

Data Storage and Backup

File Naming

(70) Keep file names short, as a rule, do not exceed 32 characters. Only use alpha numeric characters without punctuation. Files should be named with a three character extension for portability between operating systems.

Good File Naming Examples

> MyResearchFile.doc

Poor File Naming Examples

File Name	Issue
1.doc	Poor information about file
MyResearchFile	No file extension
Outcome. of: total, for year06.xls	Use of punctuation
A BLOTT Mr Andrew Technology Services (A) 2234.doc	Using standard office default
Copy of my data for my research project that is pre-compilation of field data not yet vetted by coordinator as at the third of June two thousand and five.xls	File name too long

(71) Folders backed up on a PC to File server

a. MyDocuments
b. Favourites

(72) Items not backed up on a PC to file server

a. Attachments
b. Applications/Software
c. Specialised Software and associated data
d. Windows Desktop
e. Installer Programs
f. All non-work related data

(73) Folders that are backed up on a Mac to the file server

a. Home/Documents

(74) Items not backed up on a Mac to the file server

a. Applications and Programs
b. Desktop folder
c. All non-work related data
d. Personal Data

(75) Personal data for example a resume, will be kept in a folder called Personal on your hard drive. Your personal folder will not be backed up to the file server. It is your responsibility to maintain copies of these files.

Deletion of Data

(76) If the user requires their data to remain on University servers for a given period of time. The user will request this by providing the following details -

a. Name, Faculty/Work unit and contact details
b. Statement on what is required
c. The period of time required for the data to be kept.

(77) These details should be sent to servicedesk@scu.edu.au.

Archiving and Deletion of Files

Archive Procedure for U Drives

(78) The amount of data stored on a U drive cannot exceed the allocated maximum limit. Once this threshold is met, a user must archive their data. To archive - use the following procedure.

a. Delete all personal non work related data from your U drive. This may include:
    i. Pictures
    ii. Personal Attachments
    iii. Music
    iv. Temporary files (internet cache etc.)
    v. Installer programs
    vi. Video files
b. Create a number of folders which represents the year documents were originally created on your U drive. You may wish to duplicate the original file structure under each year for ease of retrieval in the future eg:
    i. U:/ Admin
    Policy
    Procedures
    2001
        - Admin
        Policy
        Procedures
    ii. 2002
        - Admin
        Policy
        Procedures
    iii. 2003....

c. Copy all files you wish to archive under their respective years and associated folder
d. Copy each year folder (eg 2001) to a backup medium (more than one copy on different medium is also recommended)
    i. Thumb Drive
    ii. External Hard disk
    iii. CD ROM
    iv. DVD ROM
e. Test that the data is available on the backup medium
f. Delete year folders from your U drive

Printing

(79) Students will need to obtain a pre-paid services card from the dispenser units located in the Library and computing labs.

Wireless Access

(80) A wireless account is provided for all staff and students at all campuses. More information regarding wireless is available on the Wireless Services webpage and also from the Wireless Networking Security Policy.

(81) Advanced and special purpose software Information regarding software programs can be obtained through the relevant SCU Call Centre.

a. Lismore Campus - Email servicedesk@scu.edu.au or Phone: 02 6620 3698
b. Tweed/Gold Coast Campus - Email servicedesk@scu.edu.au or Phone: 02 6620 3698
c. Coffs Harbour Campus - Email coffs.servicedesk@scu.edu.au or Phone: 02 6659 3080

Software Support

(82) Information on the supported software at SCU can be found in the Standard Operating Environment (SOE).

(83) Making a complaint about Technology Services - Including Web content

(84) Any person can make a complaint by emailing servicedesk@scu.edu.au or via the Southern Cross University Complaints Management Framework. Information can be found on the Complaints and Student Ombud web page or by contacting Nominated Complaints Officers

Part M - Procedures for a Breach of the Computing Conditions of Use Policy

Knowledge and/or Allegation of Breach

(85) Any person may report an allegation that a user has breached the conditions for acceptable use of information facilities to the Client Services Manager or a delegated officer.

(86) Any person becoming aware of any action by another individual which could be considered a breach of policy, should report it to the Client Services Manager or a delegated officer.

(87) The report may be provided orally or in writing to:

Client Services Manager

Technology Services

Level 1, A-Block, Lismore Campus

Phone: 02 6620 3481

Email: infosec@scu.edu.au

Initial Steps to be Taken by Delegated Officer

(88) The delegated officer (on the delegated officer's own initiative or in response to a report) may take any of the following steps upon becoming aware of an allegation:

a. make enquiries to decide whether to proceed against a user for an alleged breach of these rules and determine severity of breach to decide whether an interim suspension to access is warranted or a caution is to be applied;
b. if practicable and warranted, remove the item/s that are the subject of the allegation
c. impose an interim suspension to access Refer to Interim Suspension, clauses (89) to (91);
d. advise the Chief Information Officer of the allegation under Part I, clauses (49) to (51) (Non-Compliance) of the Computing Conditions of Use Policy;
e. notify the University's Legal Services, if the delegated officer suspects that the user may have breached a law of the State or the Commonwealth.

Interim suspension

(89) Upon receiving a report of a suspected breach a delegated officer may impose an interim suspension of access to some or all information facilities.

(90) The delegated officer may impose an interim suspension only if the officer considers it necessary to avert a substantial risk of any of the following -

a. attempt to prevent that Misconduct from occurring; or
b. protect the health, safety and welfare of others, including the rights of other students to pursue their studies and the rights of staff to carry out their work; or
c. ensure the University and its activities can function properly.

(91) The delegated officer must advise the Chief Information Officer or nominee immediately of the interim suspension being imposed. Refer to 9.24 Breach Notice

Breach notice

(92) If the delegated officer decides to proceed against a user, the delegated officer must provide notice of the alleged breach (the "breach notice") to the Chief Information Officer or nominee outlining -

a. the relevant section of the Computing Conditions of Use alleged to have been breached; and
b. the incident or conduct giving rise to the alleged breach; and

c. evidence that the delegated officer has of the alleged breach.

(93) The Chief Information Officer or nominee will then determine future action to be taken in accordance with relevant Misconduct Rules.

Cautions

(94) A delegated officer may issue a caution as an alternative when -

a. the alleged breach is minor; and
b. the conduct giving rise to the alleged breach is not continuing; and
c. the user has not previously been reported for a breach or alleged breach.

(95) If the delegated officer decides to issue a caution, the officer is not required to issue a breach notice.

(96) The caution is issued in writing.

(97) Where a caution is issued, no other action on the alleged breach may be taken under these rules.

(98) Nothing in this section prevents a university officer issuing a direction to a user to avoid a breach.

Schedule 1

(99) Potential breaches of Computing Conditions of Use include, but are not restricted to:

a. Acts considered illegal under State or Commonwealth legislation
b. Acts not associated with teaching, research or administration
c. User use not directly related to their academic program
d. Use of another users computing account
e. Access or attempted access to facilities to which the user has not been authorised access
f. Use of facilities for profit making or commercial activities without authorization
g. Abuse or hacking of any computing or communications facility
h. Inappropriate use of email systems
i. Use of programs including, but not restricted to file sharing, internet gaming, virtual worlds, IRC and streaming audio and video programs
j. Infringement of software licensing agreements
k. Content placed on websites in the University domain contrary to Web Hosting and Publishing Policy
l. Material infringing the copyright of others

Notification to Staff and Students - Terms and Conditions Regarding Use of SCU Computers and/or Network

(100) You must take reasonable steps to protect the confidentiality of your accounts and passwords. This includes not disclosing your account details to anyone, including SCU employees.

(101) Accessing any of the following while using SCU computers and/or network (including the wireless network) is strictly prohibited and may lead to loss of access:

a. Gaining unauthorised entry to other sites
b. Pornography
c. Unauthorised streaming video, music, internet radio, online games, file-sharing

d. Gambling/Gaming
e. Violation of copyright
f. Deliberate spreading of viruses or malicious code
g. Recreational Chat.

(102) SCU computer and/or network resources are not to be used for commercial purposes without written permission from SCU.

(103) No software is to be installed into your account or on to University PCs without prior permission.

(104) You are required to advise appropriate SCU staff of any security issues or breaches of which you become aware of (refer to IT Security Incident Management Policy located at SCU IT Policies).

(105) Sending unsolicited, commercial based e-mail messages to multiple users contravenes the Spam Act 2003 and is prohibited. Bulk emails to SCU Staff and Students may only be sent for direct SCU related business by authorised staff and/or students.

(106) You are not to undertake any anti-social activities, including nuisance email, chain letters, and obscene, harassing or unwelcome behaviour 8. SCU reserves the right to monitor activities where it has cause to consider that the Security Policy and Conditions of Use policy are not complied with.

(107) Violations of these Terms of Use can result in disciplinary action.

(108) For further advice and information contact the SCU Call Centre on 66203698.

(109) REMEMBER - Please keep a copy of all your files in at least 2 locations for safekeeping and save your work constantly.

Status and Details

Status	Historic
Effective Date	14th August 2012
Review Date	14th April 2015
Approval Authority	Vice Chancellor
Approval Date	10th August 2012
Expiry Date	17th February 2019
Head of Work Unit	Naomi Downs Chief Information Officer
Enquiries Contact	Naomi Downs Chief Information Officer