

Data and Systems Security Policy

Introduction

Electronic data and its use are increasingly essential to the function of the University in providing teaching and administrative services. Ensuring the integrity of these data, the systems from which they are hosted, the uses to which they are put and compliance with statutory law is a mandatory obligation of the University, for example under the Data Protection Act.

In order to fulfil its obligations, the University will implement appropriate security procedures, policies and controls on all University supported systems and data. These apply to users of the system regardless of their physical location at the time of access, be it on site, at home or anywhere else.

This Policy is designed to protect both the University and the individual and requires the active participation of all IT users. In implementing these security controls, the University will maintain:

- **Confidentiality** – to ensure that data and systems can be accessed appropriately and only by those properly authorised.
- **Integrity** – to ensure that data and systems are accurate, up to date, have not been deliberately or inadvertently modified and that appropriate controls are in place to guard against internal and external threats.
- **Availability** – to ensure data and systems are available when and where required to support users in their role within the University.

For the purpose of this document, the term 'user' refers to any authorised person who is provided with a system logon account or who uses University owned IT equipment. This includes, but is not limited to:

- All full-time, part-time, temporary and casual staff employed by, or working on behalf of, the University or any subsidiary company
- All students studying with the University
- Contracts and consultants working for, or on behalf of the University
- Other individuals who are granted access to the University IT systems
- Users accessing University IT services from off-site locations.

The term 'data' in this context refers to all electronically stored information of any format, and any non-electronic reproductions of that data.

All data stored on University owned equipment, on external services under contract to the University or produced by persons in the employ of the University as part of their duties is considered to be owned by the University¹ and to be subject to this Policy.

This Policy was approved by the Chief Executive's Team on 9 June 2011 and supersedes all previous versions.

¹ See the Terms and Conditions for Academic Staff for more on Patents and Inventions and Copyright relating to research and teaching materials

Policy Summary Statements

1. **Use of University data and IT systems is subject to all relevant legislation, licence agreements, University Policies and other regulatory requirements.**
2. **The University requires all users of its IT systems to have authorised accounts. The individual account holder is fully accountable for all use of the account.**
3. **The University requires all users of its IT systems to have an appropriate, secret and personal password for each service accessed.**
4. **All users of IT systems are responsible for the security and integrity of data they use.**
5. **All users of IT systems are responsible for the physical security of the systems they use, both on and off-site.**
6. **Use of the University's IT Systems may be subject to monitoring and logging.**
7. **All content published on the University's internal and external web sites must conform to current legislation and good practice standards.**
8. **All users are required to comply with the Computer Use Code of Conduct.**
9. **All users are required to report any misuse of IT systems or infringement of this Policy or the associated Code of Conduct.**
10. **All IT related purchases must be made through IT Services as required by the IT Provisioning Policy.**

The use of any authorised account at the University implicitly binds the user to abide by the University Computer Use Code of Conduct and this Data and Systems Security Policy. Infringement may result in:

- a. The user's access being summarily withdrawn pending appropriate investigation and/or
- b. disciplinary action under the Disciplinary Policy and Procedure (for staff) or the Academic Regulations (for students).

1. Use of University data and IT systems is subject to all relevant legislation, licence agreements, University Policies and other regulatory requirements which include, but are not limited to:

- Copyright Designs and Patents Act 1988
- Malicious Communication Act 1988
- Criminal Justice and Public Order Act 1994
- Obscene Publication Acts 1959 and 1964
- Protection of Children Act 1978
- Police and Criminal Evidence Act 1984
- Computer Misuse Act 1990
- Human Rights Act 1998
- Data Protection Act 1998
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- Employment Code of Practice 2002
- Prevention of Terrorism Act 2005
- Terrorism Act 2006
- Police and Justice Act 2006
- Digital Economic Act 2010
- JANET Acceptable Use Policy (Joint Academic NETWORK)
- Marketing and Communications Policy
- Chest Code of Conduct
- Software Licence Agreements
- Copyright Licensing Agency Licence
- Newspaper Licensing Agency Licence
- Educational Recording Agency Licence

It is the responsibility of each individual to ensure they comply with the relevant legislation and University policies and other regulatory requirements. Ignorance will be no excuse in any legal proceedings that may arise.

2. The University requires all users of its IT systems to have authorised accounts. The individual account holder is fully accountable for all use of the account.

2.1 Authorisation to use University IT Services

Individual logon accounts for University IT systems are created in three ways:

2.1.1 Student Accounts

Student accounts are created automatically when applicant details are transferred electronically from Admissions to Student Records to create provisional student records. The authorisation for this arises from formal acceptance of an applicant on to a course (in the SITS system). These accounts are normally disabled three months after the student has left the institution, and deleted in the following year. If a student intermits, the account is disabled.

Student accounts are automatically provided with an e-mail address and access to the internet and intranet (including Portia and Moodle). Access to the student's own record on the Student SONAR system must be requested via an on-line process.

Services provided by Microsoft as part of the "Live@Edu" service remain available to students after the deletion of the University logon account. These services include e-mail and internet storage. The University holds no responsibility whatsoever for the delivery of services to students who have been de-registered. Account users are reminded that use of these services is subject to Microsoft's published conditions of use.

2.1.2 Staff Accounts

Staff accounts are created in a semi-automatic process when appropriate data are entered into the HR system. Authorisation comes from the acceptance of a contract of employment with the University. Staff accounts are disabled when a member of staff leaves the institution and are deleted three months thereafter.

These accounts are automatically provided with an e-mail address and access to the internet and intranet (including Portia and Moodle). Access to

Staff SONAR can be requested if required and is subject to approval from Academic Registry.

2.1.3 Other 'associate' accounts

Other associate accounts are created in a manual process from data stored on an associates' database. The authorisation for an associate account comes from a request from an existing senior member of staff (at least Head of Department level) and should be made via the IT Service Desk. The account will have a fixed expiry date and a maximum life of one year; renewal requires reauthorisation. The member of staff requesting the account is responsible for managing the use of that account including, if appropriate, its re-authorisation to avoid expiry.

Associate accounts are automatically provided with an e-mail address and access to the internet and intranet (including Portia and Moodle).

2.2 Generic logon accounts

A general local desktop logon is provided for use in the teaching rooms at the University. This is a restricted account designed to allow visitors to use the provided desktop or laptop computer and audio-visual equipment and to access the internet independently of the University's network. Use of this generic logon is enabled via a USB memory stick; these are available for loan against signature from the University Libraries and Conference and Accommodation Offices. The issuing office is responsible for ensuring the return of the USB memory stick.

Users must agree to comply with the Code of Conduct for Computer Use.

2.3 Resource accounts

Resource accounts are available on request (from a Head of department or above) to facilitate group working and collaboration. Such accounts are provided with an email account (including a calendar) and internet storage. The owner of the account is responsible for its proper use, and should ensure that access to the mailbox, calendar and storage are properly delegated to appropriate group members. The account is subject to the same conditions as any other account; specifically, the password should never be shared. The owner is also responsible for the transfer of ownership (to another responsible manager) and/or ultimate deletion of the account.

For example, itservicedesk@chi.ac.uk is the email address of a resource account designed to allow communication with the IT Service Desk. It is owned by the Head of Service Delivery, and access is delegated to all Service Desk team members.

2.4 Access to Corporate Business Systems

Access to specific business systems such as the Finance and Human Resources systems, detailed in Appendix A, is controlled by the Manager responsible for the system. Access to these systems requires additional authentication ("two factor authentication") and they are therefore excluded from the 'single-sign-on' service.

The responsible Manager will determine who should have access, and the level of that access, on an individual case-by-case basis. This access will be revoked when the member of staff leaves the institution or at the request of the responsible Manager.

Gaining access to University systems by any other means will be deemed to be in breach of this Policy and will be subject to appropriate disciplinary action.

3. The University requires all users of its IT systems to have an appropriate, secret and personal password for each service accessed.

- 3.1 All users must manage the password for each service they are authorised to access in a safe and secure manner:
- Each password must be unique
 - Passwords or logon details should never be divulged to any person; this includes the account holder's manager, colleagues, staff and members of IT Services
 - Passwords and logon details should be stored privately and securely; an office, even if locked, is neither private nor secure.
 - Individual users will be held accountable for activity on their own account(s).
- 3.2 To facilitate the secure management of passwords on the IT systems, the following rules are applied:
- Passwords for the main University network will automatically expire after one year; passwords may not be reused.
 - Passwords for Corporate Business Systems such as SITS (the Student Records System) will automatically expire after 90 days and may not be reused
 - Passwords on the main University network system require a minimum of EIGHT characters (two of which must numeric) with a mixture of upper and lower case characters.
- 3.3 If users need to share information which is not 'personal sensitive' or otherwise restricted with other users, there are a number of solutions available to enable this in a safe and secure manner and without the need for passwords to be divulged. For example, the "Live@Edu" system provides tools for the delegation of calendars, mailboxes and internet storage.
- 3.4 Help and advice is available from the IT Service Desk and is published on the IT Help web pages.

4. All users of IT systems are responsible for the security and integrity of data they use.

- 4.1 University data should not be made available to unauthorised persons, or for unauthorised activity. University data should never be stored on personal computers which are accessed by private individuals. Personal computers which use wireless connections should always use secure connections.
- 4.2 Application based passwords (for example in Word, Excel) should be used with care, as there is no recovery available if the password is forgotten or not available (for example due to holiday, sickness, death).
- 4.3 This policy recognises four classes of data:
- 4.3.1 *Sensitive Personal Data (including Personal Data)*
Sensitive Personal Data is data that, if released to unauthorised persons could have a significant impact on an individual. This includes any data identified by the Data Protection Act as sensitive personal data, including data relating to racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sexual life, sexuality, offences or alleged offences.

4.3.2 *Sensitive Data*

Sensitive data is data that, if released to unauthorised persons, would be likely to cause damage or distress to one or more individuals or to the University, including personally and commercially confidential documents and infringement of intellectual property rights. Any data that could be used for illegal purposes is also included.

4.3.3 *Non-sensitive data*

Non-sensitive data is data that, if released to unauthorised persons would not adversely affect any individual or have a negative impact on the University.

4.3.4 *Unauthorised data*

Unauthorised data is data that **should not be distributed** via University IT systems. Individuals have a responsibility either to remove this data or notify IT Services of its existence. This includes, but is not limited to:

- Personally owned music files
- Personally owned video files
- Personally owned photographs
- Personally owned software
- Unregistered personal data (see Data Protection Act)
- Any data that is not compliant with University Policies, Copyright Licences, procedures or current legislation.

4.4 Data and Data Storage

A variety of data storage media and locations are available; the user is required to select the most appropriate option to ensure data security, integrity and availability, taking into account the data class.

The University is responsible for the overall security management of the following storage facilities:

4.4.1 *H: drive (all staff)*

This area is provided to individuals to hold data related to University business that is personal to them. The contents will be deleted when the account holder leaves the University. The data are regularly backed up, and it may be possible to recover deleted information on request.

4.4.2 *S: drive (staff only) has both 'public' and 'private' areas:*

- *The S: drive 'public' area* is used to provide a shared file storage area. The files can be shared across the University restricted to groups and/or individuals. The files are retained when a member of staff leaves the University. The files are regularly backed up and it may be possible to recover deleted information on request.
- *The S: drive 'private' area* is used to provide secure, restricted access storage for confidential documents; each folder in this area is managed by a designated owner who controls which members of staff can access the contents. These files are retained when a member of staff leaves the University or if the individual transfers control to a successor. The files are regularly backed up and it may be possible to recover deleted information on request.
- *Encrypted Memory Sticks and other USB Storage Devices (staff only)*
From September 2011, any USB storage device used to write data from a University-managed Windows desktop PC, or Windows-based laptop PC issued to an individual as a desktop replacement, will automatically be encrypted, making it suitable for use with all classes of data.

Automatic encryption will NOT be available on PCs borrowed from Equipment Loans or on Apple Mac equipment. Staff users of these devices, or of non-University managed computers, who require access to Sensitive Personal Data and Sensitive Data from locations where access to the University Network or to the Internet is not available, should request an encrypted device from IT Services.

IT Services will be able to recover data from the encrypted devices described above should the relevant password (s) be lost.

- *Encrypted Laptop Computers (staff only)*
Hard disk encryption is implemented on University owned Windows-based laptop PCs issued to individual members of staff in place of a desktop machine. These machines are therefore suitable for use on and off-campus with all classes of data; IT Services will be able to recover data from these machines should the relevant password (s) be lost. Encryption is not currently implemented as standard on University-managed Apple Mac laptops. These may therefore not be taken off-campus if there is any possibility at all that they contain any Sensitive Personal Data and Sensitive Data.

Note that laptops borrowed from Equipment Loans do not have encrypted hard disks, and should therefore NOT be taken off-site

- 4.4.3 The University is responsible for user account management and for access to the services from the University for data storage facilities that are provided by Microsoft UK Limited as part of the "Live@Edu" service. Microsoft manages the overall service provision, including physical datacentre security and service availability. Whilst the risk of data loss under this arrangement is considered extremely low, there is no facility for deleted data to be recovered on request. These facilities should not be used for permanent storage of University data as, for staff members, all storage associated with the service is deleted when an employee leaves the University. Users should exercise caution in using this medium for the storage of Sensitive Personal Data and Sensitive Data.

- 4.4.4 The following are available:

- *SkyDrive* provides a 'virtual USB drive' on the internet. A SkyDrive is provided with every University email account, and can be configured by the user to provide both private and shared storage. It can be accessed from any location where an internet connection is available.
- *Office Live Workspace* has the same security characteristics as the SkyDrive, providing storage for Office documents in an environment suitable for personal and group access.
- *The Outlook Live email system* provides storage for email correspondence and attachments. The Live@Edu account for students and all associated storage remain available indefinitely.

- 4.4.5 *Other storage media and services*

The University holds no responsibility for other storage devices or services that individuals choose to use, and users have full accountability for their actions. Examples include but are not limited to:

- Non-University owned personal computers, laptops and netbooks
- University-owned Apple Mac laptops or loan laptops
- Tablet PCs
- CD and DVD disks

- Unencrypted USB memory sticks
- Unencrypted removable hard drives
- PDAs and mobile phones, including smartphones
- Data tapes
- External web services
- SIM cards, flash memory and MP3 players
- Games consoles
- Non-University provided email systems

Sensitive Personal Data and Sensitive Data should not be stored on these devices.

- 4.4.6 Increasingly, devices such as smartphones provide for the receipt and storage of email data. To comply with the above, users should:
- Protect their devices with a PIN code and/or password
 - Ensure that emails containing (personal) sensitive data are removed promptly from the inbox and stored in a folder that is not synchronised with the mobile device
 - Inform IT Services immediately if a mobile device synchronised with the University email system is lost in order that email data can be deleted remotely.

4.4.7 *Personal Privacy and Confidentiality*

The University acknowledges the right of its students, staff and other users of its IT Services to expect that individual privacy and confidentiality are respected at all times. The needs of the University in carrying out its core activities and the rights of others must also be respected. To this end, strict controls are enforced before any user's personal storage – including the H: drive, email storage, SkyDrive and storage on University provided personal computers and mobile phones – is accessed without the user's permission. IT Services will only arrange for such access when:

- It is not possible (or appropriate) to seek the user's permission
- An instruction in writing, detailed what access is to be provided, to whom and for what purpose, is given to the Director of IT Services or his/her delegate, and
- This instruction comes from a member of the Chief Executive's Team.

Examples of circumstances when such an instruction might be given include the death or unexpected long-term absence of a user, or a requirement arising in support of a formal University or other official investigation.

4.5 Specific Responsibilities of IT Services

4.5.1 *Access Rights*

- IT Services will ensure access rights to data on University systems are proactively managed; management access will be restricted to authorised personnel only.
- IT Services will advise corporate business system owners on best practice for access and data security.

4.5.2 *Data and Network*

- IT Services will manage appropriate access control services (firewall) to protect the integrity of data and the IT infrastructure from internal and external misuse and exploitation.
- IT Services will manage appropriate desktop security and anti-virus applications to protect individual equipment and guard against data corruption.

- IT Services will implement VLAN technology across the institution to segregate usage of network resources into secure areas protecting against data corruption and misuse.
- IT Services will apply appropriate network segregation between student and staff accounts and resources to protect against data corruption and misuse.
- IT Services will implement appropriate technology to ensure all University financial transactions undertaken using the network are secure.
- IT Services will implement appropriate back-up services for systems and data to provide Disaster Recovery capabilities and file recovery details at Appendix B.
- IT Services will implement emergency close down or other protective action if unacceptable risk to data or serious degradation of performance.
- IT Services will arrange for the destruction or irrevocable deletion of all data held on redundant University equipment (computer hard drives, printer and scanner memory, portable data storage devices, mobile telephones), ensuring appropriate certification is received from third party organisations involved in this process.
- On request, IT Services will arrange for the destruction or irrevocable deletion of data held on media such as disks, tapes or flash memory surrendered by University users.

4.5.3 *Wireless*

IT Services will manage wireless access to ensure integrity of data and provide an infrastructure supporting a range of service activity including authenticated, public or commercial access.

4.5.4 *IT Services Staff*

In order to perform their duties, certain IT Services personnel have access to accounts that allow access to data stored in otherwise secure or private areas of the infrastructure. Such personnel are required to sign a confidentiality agreement before being given responsibility for such accounts. They may be required to undertake monitoring or other investigations with appropriate authority. Breach of trust in this area will be subject to disciplinary action. In line with the requirements of paragraph 4.4.7, Personal Privacy and Confidentiality, monitoring and/or investigation will require a written instruction, with details of the requirement and the reasons, from a member of the Chief Executive's Team.

5. All users of IT systems are responsible for the physical security of the systems they use, both on and off-site.

- 5.1 Users should undertake all reasonable measures to prevent unauthorised persons from accessing University data and systems, or introducing viruses or malware.
- 5.2 University computer workstations should be logged off, or be in 'locked workstation' mode when not in use or left unattended. IT Services will implement an automatic 'locked workstation' mode after five minutes of inactivity.
- 5.3 It is a mandatory requirement that any mobile device owned by the University with Sensitive Personal Data or Sensitive Data on it should have appropriate data encryption enabled. Appropriate use should also be made of inbuilt security features such as PIN numbers and lock codes on mobile phones and BIOS and hard drive passwords on laptops, and these devices should never be left unattended in an insecure area.

It is a breach of the Data Protection Act to take equipment, which holds Sensitive Personal Data or Personal Data off University premises unless it is on a device that has data encryption enabled.

Sensitive Personal Data or Sensitive Data should never be installed on non-University owned equipment.

- 5.4 Users should never divulge passwords or other account access information to any third party.
- 5.5 Users should never allow access to computer systems logged on with their own credentials to any other user.
- 5.6 Users should not attach or otherwise introduce unknown electronic devices, such as PDAs, USB memory sticks, DVDs, mobile phones, CDs to the University IT Services network.
- 5.7 Users should not include or attach Sensitive Personal Data or Sensitive Data in emails to unknown recipients or recipients who do not have authorisation to receive this type of data.
- 5.8 Users should exercise caution when connecting to wireless networks. Any network, which does not require authentication via a user id and password, should be regarded as insecure; users should not connect to networks of unknown ownership.
- 5.9 Users should notify IT Services immediately if any University owned data storage device, such as USB stick, laptop, mobile phone, or PDA, is lost or stolen.

Remember: in accordance with Data Protection legislation, you are personally liable for your actions and their consequences; these could include both financial and reputational damage to the University.

5.9 Specific responsibilities of IT Services are:

5.9.1 *Server Rooms*

- IT Services will control access to University server rooms and record every access made to each room.
- All IT equipment, including servers and switches located in a server room requires appropriate authentication for access. This authentication should be unique for each system.

5.9.2 *Servers*

- IT Services will implement automatic time-out server connections after a period of inactivity

5.9.3 *Wiring Centres*

- IT Services will control access to wiring centres located in each building.
- All equipment located in a wiring centre will require appropriate authentication for access.

5.9.4 *Telephony*

- Where telephony equipment co-resides with IT equipment in a server room or wiring centre, IT Services will control access to that location.

5.9.5 *Infrastructure*

- IT Services will ensure appropriate inter-building and inter-site connections are secure from damage and misuse.

5.9.6 *Security Patching*

- IT Services will manage the application of security patches to University IT equipment to ensure data security and integrity in line with current best practice.
- Patches applied to servers will be tested on an off-line system prior to release on live systems
- Critical or other high security patches on desktop and laptop operating systems will be applied automatically on release by the vendor.

5.9.7 *Desktop Systems*

- IT Services will manage the automatic process on the desktop systems to ensure workstations are locked after a period of non-use.
- IT Services will automatically disconnect applications after a period of non-use.

6. Use of the University's IT Systems may be subject to monitoring and logging.

6.1 IT Services will routinely monitor the status of IT systems to assist in the management, protection and development of these systems. The aggregate level information from this monitoring will only be used internally within IT Services.

6.2 Automated logging processes at a more detailed level are also in place. This logging produces data files that are stored securely, and are not accessed in any way unless instructions to do this are given with appropriate authority. Such instructions must be provided, with details of what is to be done and why, by a member of the Chief Executive's Team or the University Secretary. This may happen in the following circumstances:

- A request is made by the security forces
- A request is made by a police force investigating alleged criminal activity, or in support of other law enforcement processes
- The University is undertaking an internal investigation in line with its published Policies and Procedures
- The University is required to provide information to external bodies such as a software licensing company in line with the terms and conditions of a licensing agreement
- The Chief Executive's Team determines that monitoring or investigation is necessary to ensure compliance with the law or with University Policies and Procedures.

7. All content published on the University's internal and external web sites must conform to current legislation and good practice standards.

7.1 Accessibility

All web pages should be designed to comply with the guidelines published by:

- WCAG (Web Content Accessibility Guidelines)
- W3C (World Wide Web Consortium)
- WAI (Web Accessibility Initiative)

and comply with the following legislation:

- SENDA (Special Educational Needs and Disability Act 2001)

7.2 Web content management

- The overall management of the University's websites is governed by the Digital Communications Strategy
- Templates and style sheets are provided by Marketing for the design and layout of both internal and external web pages and should be used for all content.

7.3 Content

- Content owners and/or editors who deploy content to the Intranet, Public Web site or any other web site in the chi.ac.uk and chiuni.ac.uk domains are wholly responsible for the accuracy timeliness and compliance of their content.
- Web pages must not include illegal, offensive, threatening or harassing material, or anything that constitutes a criminal offence such as breach of copyright.
- Web pages should not knowingly link to other web pages that contain illegal, offensive, threatening or harassing content.
- Access from the University to the Internet site is via JANET and use must comply with the JANET Code of Conduct. This explicitly excludes commercial use other than the promotion and publicity of the institution.
- All personal information is subject to the Data Protection Act and can only be used on a web page with the consent of that person.
- All content contributors should ensure that all information is up-to-date, accurate, proof read and spell checked prior to publication.

7.4 Content contributors should at all times remember that they are promoting the University's image and reputation worldwide and should adopt good practice in providing a high quality service.

7.5 Detailed requirements for all web sites, electronic communication, publications and presentation of the Corporate Identity can be found in the Marketing and Communications Strategy.

8. All users are required to comply with the Computer Use Code of Conduct.

9. All users are required to report any misuse of IT systems or infringement of this Policy or the associated Code of Conduct.

9.1 Users must report any misuse of IT Systems or infringement of this Policy to the Director of IT Services for further investigation.

9.2 If for any reason this is not appropriate, then the University's Public Interest Disclosure Policy and Procedure is available from HR, the HR pages on Portia, the University Secretary and the Policies section on the Governors' web pages.

10. All IT related purchases must be made through IT Services as required by the IT Provisioning Policy.

10.1 In order to provide a secure and stable environment, IT Services needs to control, monitor and maintain the software and hardware systems deployed by the University. Requests for software, hardware and related items should be made in line with the IT Provisioning Policy, to be found at <http://help.chi.ac.uk/ITProvisioningPolicy.cfm>

10.2 This is in order that:

- Software is suitable for use on the University network, correctly licensed, recorded on the software register and has an appropriate maintenance plan which includes security updates
- Hardware is safe and secure, compatible with the existing infrastructure, recorded on the equipment register and has appropriate maintenance and replacement plans.

Computer Use: Code of Conduct

(To be read in conjunction with the Data and Systems Security Policy)

The University has an obligation to ensure that computing services, (hardware, software, network services) are used appropriately in support of institutional activities and to ensure compliance with statutory provisions and licence agreements.

Computing services and facilities are provided to enable staff, students and guests to carry out their work, research or studies while at the University. On activating an IT account at the University, the user is explicitly bound by this Computer Use Code of Conduct and the associated Data and Systems Security Policy.

General Computer Use

1. All users of computing services at the University must comply with the Data and Systems Security Policy.
2. Users should not intentionally cause damage or otherwise jeopardise the integrity of computer equipment, software or network services.
3. Users must not knowingly introduce computer viruses to the computer systems, and should take all precautions to prevent their spread.
4. Users must abide by all agreements and contracts by which software and datasets are accessed at or through University computing services. Specifically, users must not install, replace or update any software or dataset on University computing equipment without appropriate authority.
5. Users must not move, alter, connect or install hardware into/onto University computing equipment without appropriate authority, (this includes taking equipment off-site).
6. Users must not use any University computing services to gain unauthorised access to any other computing system (internal or external).
7. Users must not use University computing services for storing, receiving or transmitting offensive, indecent or obscene material. If there is a genuine academic need to use such material, this should be approved by the Head of Academic Department in advance and arrangements for their access then made with IT Services.
8. Users must not use University computing services for any commercial activity without appropriate authority from IT Services.
9. Users are not permitted to use the computing services for private commercial purposes or any other employment outside the scope of that person's official duties or functions.

Appendix A Specific Service Access

Access and levels of authority owned and managed/authorised by:	Systems
Director of Admissions and Academic Registry	SITS student and applicant records system where relevant to student records.
	Staff SONAR – web student and applicant records system where relevant to student records.
	SASS Archive student and applicant records system where relevant to student records
	SITS student and applicant reporting system (Slreporting) where relevant to student records
	Student Handbook management system
	SITS student and applicant records system where relevant to applicant records
	Staff SONAR web and student applicants system where relevant to applicant records
	Admissions Portal applicant management portal
Web enquiries Prospectus and on-line course database management system.	
Head of Academic Quality and Standards Unit	External Examiners Database
Director of Estate Management	Forum conference and Student Accommodation System
	Accession and Records Register
	Parking Permits Database
Head of Finance	QLX Finance System
	Finance Reporting System (Qlreporting)
	QLX Online Budget Reporting System
	Online Payments WPM management screens
	Online Purchasing System
Director of HR	[ADD CURRENT AND NEW SYSTEMS???
Head of Library Services	Talis Library Management system
Director of Marketing, Communications and Access	Open and Taster Day web and database management system.
Head of IT Service Delivery	User Status Database tool for student account management.
Head of Student Support and Careers	Student Services management and recording system
	Student Handbook management System

Appendix B Back-up Service Detail

1. The IT Operations team runs frequent data back-ups for every critical, network-based service hosted on the University infrastructure. The back-up policies are designed to preserve data in the event of a disaster or other unplanned event causing damage affecting IT Services. Data can then be restored and the affected service(s) can be reactivated for user access.
2. There are three different back-up regimes designed to serve all of the services the University provides in an efficient manner that optimises the use made of available fast, online (staging) storage. These are:
 - Network based drive back-ups (a copy of an entire server on another part of the network)
 - Network based file level back-ups (a copy of specific files on another part of the network)
 - File based tape back-ups (a copy of specific files onto tape).
3. All of the above are equally robust, and they have also been tailored to suit the University's infrastructure. The Operations team has performed a number of different tests on each of these types to ensure their reliability in the case of a real disaster.
4. Back-ups of volatile data are run every weekday evening. No back-ups are performed at the weekend or on public or University holidays.
5. The standard back-up routine is to "stage" a copy of the data on a high speed storage server overnight and then to transfer the data to tape. The advantages of this process are:
 - 5.1 Disruption to service is minimised as disk to disk file transfers offer better performance than use of tape.
 - 5.2 Slower speed disk to tape transfer is performed "offline" with no disruption to the service.
6. The standard back-up routine is as follows:
 - *Daily back-up* – back-ups each night of the week. These are short-term back-ups (see table below) and tapes are re-used regularly.
 - *Weekly back-up* – full back-up of data once a week. This data is kept for the duration specified in the table below.
 - *Monthly back-up* – full back-up of data once a month (usually the last day of the month). These tapes are kept for the duration specified in the table below. The length of time a back-up is retained greatly depends on the service that is being backed up, the table below shows which services are included in the back-up plan and how long back-ups are retained.

Service Type	Daily Back-up	Weekly Back-up	Monthly Back-up
Staff and Student Data			
Staff H: Drive	5 nights	4 weeks	6 months
Student H: Drive	5 nights	4 weeks	6 months
Staff S: Drive	5 nights	4 weeks	6 months
Staff G: and R: Drive	5 nights	4 weeks	6 months
Application Data	5 nights	4 weeks	6 months
Mac Student H: drive	n/a	n/a	n/a

Service Type	Daily Back-up	Weekly Back-up	Monthly Back-up
Corporate Systems			
Forum	5 nights	4 weeks	6 months
SITS	5 nights	4 weeks	n/a
QLX	5 nights	4 weeks	n/a
CIPHR	5 nights	4 weeks	n/a
MidlandHR	?	?	?
SupportWorks	14 nights	2 weeks	n/a
Web Servers			
Moodle	14 nights	2 weeks	n/a
Portia	14 nights	2 weeks	n/a
ChiUni Website	14 nights	2 weeks	n/a
Web Database Content	14 nights	2 weeks	n/a
Accommodation Network			
Bognor Accommodation Service	14 nights	2 weeks	n/a
Chichester Accommodation Server	14 nights	2 weeks	n/a

For example, for the H: drives, back-ups will be held for:

- Every day in the last working week
- Every Friday for the last month
- The last day of every month for the last six months

Back-ups are mostly stored on a removable tape which is stored in a separate location from the service that it protects. This is either in a remote server room, or in a fireproof safe on campus, with a recent back-up set from the Chichester data centre held at Bognor Regis for use in a major emergency. In many cases, data are first backed up to a staging area, for performance reasons. These back-ups are subsequently moved onto tape.

The restoration of user data that are accidentally deleted, corrupted or otherwise damaged can be requested from the IT Service Desk. Restores will be performed on a best efforts basis; users should take into account the policies described above and note that, in general, the older the data, the less likelihood of successful recovery.