Information Services Policy & Guidance

Information Services

Information Systems Policy

Document Reference: ***Final Version 1.3***

December 2012

CONTENTS

1. Purpose

This policy establishes the direction, procedures and requirements to maintain the security, confidentiality, integrity and availability of University information, communication and computing services. It explains what is classified as the acceptable and unacceptable use of the information systems at Glasgow Caledonian University.

2. Organisational scope

This policy applies to all persons and processes using information, communication, computer systems and applications owned by, developed or installed within and by the University.

3. Definitions

Access Control: A mechanism by which a system, process or person grants or revokes the right to access information, or perform an action.
Application: Software that performs a specific task or function.
Authentication: A process to verify the identity and permissions of an individual, such as a request to log-in to an information system.
Backup: Making copies of information so that these additional copies may be used to restore the original after a loss of information.

Business of the University: is defined in the University Strategy as the mission and vision, refer to *http://www.gcu.ac.uk/theuniversity/aboutglasgowcaledonian/vision/ourmissionvision/*

Computing Facilities: Information systems designed to facilitate and enhance the academic programmes and business needs of the University.
The Information Technology facilities provided by the University comprise all computer hardware and software (including for example printers, photocopiers, scanners, PDA"s, network equipment etc) as well as all audio visual equipment (such as cameras, tripods, data projectors, overhead projectors etc).
Data Centre: A facility approved by the University to house information systems and associated components, such as telecommunications and storage systems.
Electronic Messaging: Systems for the delivery of text or graphically formatted electronic messages.
E-Mail: Short for electronic mail. E-mail is a store and forward method of composing, sending, storing, and receiving electronic messages.
Encryption: The process of converting information into cipher or code in order to maintain confidentiality.

Filtering: A filter is an information system designed to process an information stream and permit or deny access dependent on the content or address.

Hardware: A physical computer system, peripheral or component.

Information System(s): Any technology based information processing system.

Internet: A worldwide, publicly accessible set of interconnected information systems.

IT Helpdesk: A single point of contact for all information technology incidents.

JANET: Is the network operating group that manages the education network on behalf of the education institutions in the United Kingdom.

Laptop: A portable computer designed to function in the same manner as a standard desktop computer.

Malicious Software: Any software intended to cause harm to or facilitate unauthorised access to an information system.

Media Access Control (MAC) Address: A Media Access Control (MAC) address is a quasi-unique identifier attached to most computer network devices.

Network(s): An interconnected set of Information Systems.

Remote Access Service: A service provided to facilitate remote access.

Remote Access: Accessing Information Systems from a network external to the central University system(s).

Risk: The chance of something happening that will have an impact on the achievement of the University‟s objectives. Risk is measured in terms of consequences and likelihood.

Software: Applications and programmes designed to perform tasks on an Information System.

Spam: unsolicited email sent to many users to advertise a product or communicate a cause.

Spyware, malware or key-loggers: Programmes to track an individual‟s use of a computer without their knowledge. The information is then used at a later stage to gain unauthorised access to their information.

Virtual Private Network (VPN): A virtual private network (VPN) is a private communications network tunnelled through another network.

Wireless Network(s): Any network whose interconnections are implemented without the use of wires

4. Responsibilities of Information Users

4.1 Acceptable use of Information Systems

4.1.1 Breach of the terms of this policy will normally be a disciplinary offence. Each member of staff/student is deemed to accept the whole terms of this policy by virtue of their acceptance of its terms, when logging on to the system, whether they did so immediately prior to any breach or

some time previously. Breach of this policy will be dealt with in terms of the University's Discipline Policy & Procedure. Guidelines on acceptable reasonable use of information technology and infrastructure are found at Appendix Three. Any breach of the clauses contained in this policy is considered an information security breach and must be reported to the Head, Infrastructure Contracts and Data Security immediately it is identified by a staff member or student.

4.1.2 Any investigation in terms of the University's disciplinary policy may include the production of soft copy or hard copy prints of the files or attachments or of pages from the relevant websites that are the cause of the breach. The copy of such files or attachments may be retained by the University and used in evidence in any disciplinary hearing or any subsequent employment tribunal application that may follow.

4.1.3 The University encourages the use of the Internet, e-mail and other Information systems and is committed to acting in compliance with individual‟s rights under both the Human Rights Act 1998 and the Data Protection Act 1998.

4.1.4 Information systems are provided for the purpose of, learning, teaching research, engagement and administration. Use of information systems is subject to relevant University policies and conditions which are designed to maintain the confidentiality, integrity and availability of information.

4.1.5 Use of computing facilities is subject to relevant policies and conditions which are designed to maintain the accommodation in good order and to generate an academic and administrative environment that is productive, ethical, legal, secure, facilitative and effective.

4.1.6 In order to ensure that information systems function in a secure, efficient and effective manner, the University reserves the right to examine any information on its facilities and to monitor use. In terms of the Regulations of Investigatory Powers Act 2000 the University is authorised to monitor its e-mail and Internet systems in the circumstances set out in the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and it shall do so.

4.1.7 Staff must not save files that contain personally identifiable information (i.e.: names, addresses, telephone numbers, etc and other personal details) to any storage format (other than the University Network) that is unencrypted. The University has an encryption process for laptops, desktops and mobile devices. Staff who require their storage format to be encrypted should contact the IT Helpdesk. Personally identifiable information may only be used for the business of the University and under the auspices of the University Data Protection Guidelines.

4.2 Privacy

4.2.1 Staff and Students should be aware use of any Information system provided or facilitated by the University cannot be completely private as authorised users may access this information. All students and staff using the University‟s Internet and e-mail facilities must comply with the policy

and the Acceptable Use Policy for the Joint Academic Network (JANET) found at www.ja.net/company/**policies/aup**.html .

4.2.2 Disclosure of information stored by the University to internal or external parties may only be authorised by the Principal or their nominee, or a delegated authority or the individual owner of the information, or may be pre-approved where required by law.

4.2.3 Authorised Users

Persons authorised to use University information systems are:

- Students enrolled in the University
- Staff employed by the University
- Visitors to the University authorised by an existing staff member
- Other persons having special authorisation from the Principal or a delegated nominee.

4.3 Proof of Status

4.3.1 A current University identity card is proof of identity for use of student computing facilities. A University identity card should be carried at all times when using on campus student computing facilities. Failure to produce a card when requested by security officers and/or University staff may result in being requested to leave.

4.3.2 Authentication

No attempt should be made to avoid authentication. Users must not use another user‟s identification reference or password or allow another user to use their password or identification reference.

4.3.3 Inappropriate activity involving other users‟ files

Users must not delete other users‟ files or interfere in any way with the contents of their directories.

4.4 Acceptable Use

4.4.1 The University encourages individuals to use information systems for University purposes only. Personal use, private consulting work, computer games and other non-University activities should be limited and not in breach of University policies, and for employees this should not be undertaken whilst on duty. University information systems may only be used with prior authorisation. Information systems may only be used for the purpose that they have been provided and not for other purposes. Reasonable private use is permissible providing it is not associated with any illegal or discriminatory activity and does not adversely affect the good reputation of the University.

4.4.2 Limited, occasional or incidental use of the internet or storage systems for personal or non-academic purposes is understandable and acceptable where such use does not contravene this policy. However, in allowing this, the University requires staff and students to act responsibly. Staff must never allow use of this facility to interfere with their job performance or work responsibilities. Staff and students who abuse this privilege will be subject to disciplinary action.

4.4.3 If staff or students use a University Information system to carry out on-line transactions, Glasgow Caledonian University takes no responsibility for any part of the transaction and is not liable for any failure of security that might occur as a result of the transaction. The University will keep the use of this facility under review and reserves the right to withdraw the facility.

4.5 Personal Conduct

Conditions of use for hardware and software

4.5.1 Damage

Users must not in any way deliberately cause any form of damage to Glasgow Caledonian University"s information technology equipment or software, or to any of the rooms which contain that equipment. The term „damage" includes modifications to hardware and software which, whilst not permanently harming the hardware or software, incurs time and/or cost in restoring the system to its original state. Any costs associated with repairing or replacing deliberately damaged equipment or software and/or in providing temporary replacements will be determined by the Chief Information Officer. These costs will be sought from the person who has caused the damage.

4.5.2 Compliance with Instructions and Regulations

Users must comply with any instructions or regulations displayed alongside computing facilities.

4.5.3 Consumption of Food and Drink and smoking on campus

Eating is not permitted in any student computer lab. Students may drink bottled water. Eating and drinking is permitted in the Learning Café and on the ground floor of Saltire Centre. Smoking is not permitted on campus.

4.5.4 Respect Others

Users must respect the rights of others and should conduct themselves in a quiet and orderly manner when using IT facilities. Users must not occupy a computer workstation unless they are actively using it for learning, teaching and research.

Users shall not leave their belongings at a workstation in an attempt to reserve the workstation while they are away for an extended period. This is applicable in all computer labs, the Learning Café and the Saltire Centre. Not only do users risk the theft of belongings, it is also preventing the use of the equipment by other users.

4.5.5 Playing Computer Games

The playing of unauthorised computer games not associated with learning, teaching and research purposes is not permitted.

4.5.6 Removal of Equipment

No equipment should be moved from its designated place or be tampered with in any way without approval of the relevant staff member in charge of the asset. This includes changing workstation characteristics.

4.5.7 Interference with Print outs

Interference with or removal of print outs from a University Printer which belong to another person is not permitted.

4.5.8 Information Security

Accounts to access University information systems are for the exclusive use of an authorised individual and must not be used by others. Every reasonable precaution should be taken to ensure that passwords, accounts and information are adequately secured.

Staff/Students are not permitted to use the Internet to download software that has not been purchased (other than for trial purposes in accordance with the relevant license agreement), entertainment software or games, to play against others (or computers) across the Internet or participate in online gambling or gaming. Staff/Students must not download and/or install software which may be used to detect concealed settings on the University‟s network in order to determine staff/student passwords or to enable unauthorised access into University or other systems, nor use any form of device to do so. The attempt to install spyware, malware or key-loggers on any computer is prohibited.

Staff/students must respect the confidentiality of other people‟s electronic communications and may not attempt to read, gain unauthorised access to the University‟s systems or other people‟s logins, folders or files, or “reveal” passwords without approval, or seek to breach computer or network security measures, or access or monitor electronic files or communications of other staff/students or third parties.

4.5.9 Copyright

Individuals should take care that they do not breach copyright law in their use of information systems, for example by:

- Downloading copyright protected material from the Internet.
- Accessing, installing or executing copyright protected material which is not legally obtained.
- Attempting to duplicate copyright protected software provided for use on University information systems.

Penalties for breaching copyright law are great and the user may be liable for any such breach.

4.6 Unacceptable Usage of Information Systems

4.6.1 It is unacceptable to access, archive, store, distribute, edit or record sexually explicit or other offensive material. The display on any IT equipment (whether belonging to the University or the Member of staff/Student and connected to the University network) of any sexually explicit image or document is in breach of this policy.

4.6.2 The University"s Information facilities may not be used for knowingly accessing, transmitting, retrieving, viewing, downloading or storing any communications or material:-

- of a discriminatory or harassing nature (actual or potential), either in itself or to any particular individual or group;
- of a racial, religious, homophobic, or sectarian nature;
- which are derogatory to any individual or group or might be so considered by such individual or any member of such group;
- which are unlawful, offensive, indecent, obscene or pornographic or which pose a risk to the University that they may be regarded as such by any person. For the avoidance of doubt refer to the guidelines on reasonable use of Information Technology.
- which are defamatory to any individual or group, or which contains any defamatory material;
- which are contrary to the University"s Equality and Diversity Policies;
- which is designed or is likely to cause annoyance, inconvenience or anxiety to any individual or group;
- in which a member of staff knowingly or recklessly obtains or discloses to another person personal data without the consent of the data controller;
- which may be used to launch an attack against the University systems:
- for any purpose which is illegal, immoral, against any of the University"s Policies or contrary to the University"s interest.

4.6.3 If there are any queries about the above section, particularly where research or learning and teaching activities is required in any of the above areas, it is advisable to contact the IT Helpdesk for advice on how to proceed. Authorisation through the Pro Vice Chancellor (Research) or Pro Vice Chancellor (Learning Innovation) may be granted where bon-fide research is to be conducted or course requirements met.

4.6.4 Information Services, in conjunction with Schools and Departments, has developed and acquired numerous application systems for use within the University. Under no circumstances should such application system software be copied or modified without the express permission of the Chief Information Officer.

4.6.5 The use of any file-sharing, Peer-to-Peer, or similar system on any University network is strictly forbidden unless associated with legitimate learning, teaching and research activities and not associated with breaching copyright protected materials.

4.6.6 In any event the Internet should not be accessed to review material or obtain information, which could or would serve to bring the University into disrepute or amount to a criminal or illegal activity.

4.7 Private and commercial use of Facilities

4.7.1 The use of any of Glasgow Caledonian University‟s IT facilities for commercial gain or for work on behalf of other groups is not permitted unless prior agreement has been made with the Chief Information Officer because of the implications of such use on the University agreement with the JANET network. An appropriate charge for that use will be determined and agreed before any work can be carried out.

4.7.2 Unless the prior approval of the Chief Information Officer has been obtained, individuals may not establish network connections to University information systems.

4.7.3 Access to any University information system will only be granted after the individual has obtained a staff or student number or temporary access approval via the IT Helpdesk.

4.7.4 Access to any University computing facility will only be granted after the Information Policy and the associated form has been signed or electronically acknowledged by the requesting person.

4.7.5 All employees and contractors should be given access only to those information systems and computer facilities that they need in order to perform their job or complete contracted tasks. Any attempt to access other systems without prior University permission is prohibited and may result in disciplinary action.

4.7.6 All employees and contractors are required not to disclose any information they have discovered in the course of working on an Information System to any other person unless it is associated with an investigation of a breach of this policy or approved by the Principal or Principal‟s nominee.

4.7.7 Upon termination or expiration of employment, or the contractual arrangement, access to all information systems should be revoked. On commencement of a subsequent employment, or contractors‟ arrangement all access should be reviewed and updated or revoked where necessary, with access granted only to information systems required to fulfil the requirement of their new position, or contracted tasks.

4.7.8 Access to data centre areas is granted only to authorised staff with a clear need to access the facility. Only those authorised by the Head of Infrastructure and Contracts are to be granted access to data centres.

4.7.9 University information systems are provided for current University staff and enrolled students. Students and staff from other Scottish Universities and Colleges may be granted access on a

reciprocal basis as agreed by the University. Applicants must be current enrolled students or staff and provide adequate supporting documentation from their University justifying access. Such documentation should be provided by the Academic Registrar (or equivalent position) of the University in which the student is currently enrolled, and the delegated authority for staff from other Universities.

4.7.10 Subject to provisions of this policy, Visitor accounts may be created at the University‟s discretion and in some circumstances for a limited time only. Visitor accounts must only be issued once an application for an account has been approved. Line Managers should fill in the web based **Authorised Guest Form** which can be found at http://www.caledonian.ac.uk/staff/it/usersetupforms/ on the Information Services Staff IT Pages. On completion of this and email acceptance of the Information Policy, access to University information systems will be processed.

4.7.11 Individuals using University remote access systems must comply with the „Remote Access Use‟ section of this policy as amended from time to time.

4.7.12 Individuals using University electronic messaging systems must comply with the „Electronic Messaging Use‟ section of this policy as amended from time to time.

4.7.13 Individuals using University Internet access must comply with the „Internet Use‟ section of this policy as amended from time to time.

4.7.14 All individual‟s passwords must be changed each semester. The password must not be the same or an iteration of the previous semester‟s password.

4.8 Electronic Messaging

4.8.1 University electronic messaging systems are not intended for personal use. Reasonable private use is permissible providing it is not associated with any illegal or discriminatory activity and does not adversely affect the good reputation of the University. Personal use of mobile devices must be reimbursed to the University in accordance with the University‟s financial regulations.

4.8.2 Any expression of personal opinion must not be made in such a way as to appear to be representative of the University.

4.9 Unsolicited Electronic Communications

4.9.1 Unsolicited material which is circulated internally or externally, which has its origin internally or externally, may be classified as spam if it is not directly related to the University‟s learning, teaching and research activities. Unsolicited commercial marketing e-mails and electronic messages are spam.

4.9.2 Any Member of staff or Student who is found to be the originator of a spam attack from within the University or using University equipment will be subject to disciplinary action by the University. The generation of such material and its propagation using the JANET network would result in the disconnection of the University from the academic network. This would have a severely detrimental effect on University operations and on the credibility of the University, its staff and its students.

4.9.3 No e-mail or other electronic communication may be sent which attempts to hide the identity of the sender, or represent the sender as someone else.

4.9.4 The following confidentiality statement (or similar) will be added at the end of each outgoing *email: "This email is confidential, may be legally privileged, and is for the intended recipient only. Access, disclosure, copying, distribution, or reliance on any of it by anyone outside the intended recipient organisation is prohibited and may be a criminal offence. Please delete if obtained in error and email confirmation to the sender. The views expressed in this email are not (unless clearly intended otherwise) necessarily the views of Glasgow Caledonian University."*

Please see Appendix 2 which deals with Best Practices for the Use of electronic communication.

4.10 Internet

4.10.1 All individuals wishing to establish a connection to the Internet using University information systems must authenticate themselves at a filtering mechanism prior to gaining access. Security controls and other restrictive mechanisms may apply to University internet access. No attempts to circumvent such mechanisms may be made, and breaches may result in disciplinary action. An individual may request access to certain filtered sites for the purposes of teaching, learning, research, engagement and administration, with the granting of such access being at the University"s discretion through the Pro Vice Chancellor (Research) or Pro Vice Chancellor (Learning Innovation).

4.10.2 Unless the prior approval of the Chief Information Officer has been obtained, individuals may not establish Internet or other external network connections that could allow access to University information systems and/or networks and University information.

4.10.3 In order to manage the impact of excessive usage, certain restrictions and controls are required and may be implemented by the Chief Information Officer. Excessive or unreasonable use is discouraged.

4.11 University Telephones

4.11.1 Limited, occasional or incidental use of fixed (non-mobile) telephones for personal or non-academic purposes is understandable and acceptable where such use does not contravene this policy. However, in allowing this, the University requires staff / students to act responsibly. Staff must never allow use of this facility to interfere with their job performance or work responsibilities. Staff/students who abuse this privilege will be subject to disciplinary action.

4.12 International Communications

4.12.1 It is not acceptable for staff or students to use the University's telephony or communications systems to make personal international calls.

4.12.2 Use of University supplied mobile phones must also comply with this policy and relevant laws, for example Road Traffic Laws.

4.13 Network Access Control

4.13.1 University networks shall be kept logically separate to ensure that the principle of least privilege is adhered to.

4.13.2 No external network connections may be created within the University network without prior authority from the Chief Information Officer.

4.13.3 No servers may be connected to the University networks without the authority of the Head of Infrastructure and Contracts. Unauthorised servers detected on the University networks will be disconnected.

4.13.4 To ensure identification of individuals and information systems, a register should be maintained of Media Access Control (MAC) addresses. Access to the University network from a computer with that Media Access Control (MAC) address should be allowed only if the address is recorded within the register.

4.13.5 Content or information must not be hosted on University information systems accessible from the internet without prior Information Services permission. Any associated risks with this content must be recorded within the risk register (as described in the Information Security section of this policy).

4.13.6 Server systems are to be provisioned in a network protected from user networks and the Internet by an appropriate network access control mechanism, unless authorised by the Manager, Information Security.

4.14 Equipment loans

4.14.1 Borrowing Equipment

Other than in the Saltire Centre, no equipment or software may be borrowed without the agreement of the Dean of a School, Head of Department or Division or Chief Information Officer. Any software or equipment borrowed as part of a formal loan scheme or for the duration of a particular project must be returned on the date agreed at the time the loan was made or fines will apply at a level up to the cost of the equipment/software borrowed.

Users shall note that the laptops borrowed from the Saltire Centre are covered by a specific borrowing agreement which means that the borrower is liable for the full replacement cost of the laptop if the laptop is damaged, mislaid or stolen.

4.14.2 Security of Borrowed Equipment or Software

All reasonable care must be taken to ensure the security of any equipment or software borrowed. Borrowers are advised to effect additional insurance for such equipment while in their possession.

4.14.3 On leaving employment with the University, staff must notify the IT Helpdesk five days before their final day of employment if they have a University mobile phone device or Laptop. The Information Services staff will make arrangements with the line manager of the staff member to collect the devices on their final day on campus or of employment, whichever is the earlier.

4.15 Charging

There may be a charge for use of certain facilities. Failure to pay outstanding charges may result in withdrawal of services and/or withholding of awards.

4.16 Disclaimers

Glasgow Caledonian University accepts no responsibility for the malfunctioning of any equipment or software, failure in security or integrity of any stored program or data or for any loss alleged to have been caused whether by defect in the resources or by act or neglect of Glasgow Caledonian University, its staff or agents.

4.17 Remote Access

4.17.1 The Chief Information Officer or delegate shall ensure systems are provided to grant individuals remote access to information systems to support the Universities learning, teaching and research, commercial activities, community engagement and administrative functions.

4.17.2 All University policies as amended from time to time relating to the use of information systems, including regulations on ethical and legal use of University hardware, apply whilst using a remote access service.

4.17.3 The use of a particular item of software through a remote access service should be consistent with the license agreement for that software.

4.17.4 All individuals using University remote access services should be aware that information saved to information systems which are not a part of the University system may be lost. Individuals should perform regular backups to ensure the ongoing availability of such information.

4.17.5 All individuals using University remote access services must not attempt to circumvent any security controls, including encryption or filtering mechanisms. Breaches may result in disciplinary action.

4.18 Breaches

4.18.1 The University may be required to report or disclose breaches and individual actions and information to an appropriate law enforcement agency or other legal body.

4.18.2 Individuals should be aware the University may consider breaches of this policy or failure to adhere to by its terms as an act of misconduct and disciplinary action may be taken.

4.18.3 Depending on the severity of the breach the University may determine that serious misconduct has occurred.

4.18.4 Disciplinary action may include but is not limited to:

- Counselling; and/or
- Actions as provided within this policy; and/or
- Actions as provided within employment contracts, employment agreements and associated University policies; and/or
- Actions as provided within University Statutes; and /or
- Criminal charges or civil action.

5. Responsibilities of Information Professionals and Identified University Staff

5.1 Information Technology Governance

5.1.1 Executive Director of Finance is responsible for maintaining:

- Appropriate governance structures for the implementation of the objectives identified in the five-year, annually rolling strategic plan for information systems, technology and processes.

5.1.2 Chief Information Officer is responsible for:

- Maintaining and reporting on key performance indicators demonstrating the performance of information systems and processes as identified by the Executive Board.
- The implementation of the objectives identified in the five-year, annually rolling strategic plan for information systems, technology and processes.

5.2 Application and Information Systems Development

Project Proposals, Requests for Tender and Project Plans should be assessed by the Head of Infrastructure and Contracts to ensure that:

- Appropriate security measures have been taken for any proposed implementation.
- The range of available sources have been reviewed, i.e.: internal, external (i.e.: built in-house, hosted externally, or shared).
- Appropriate architectures for resiliency and redundancy and cost management are used.
- Identified security risks with new applications or information systems must be recorded in the risk register (as described in the 'Information Security' section of this policy).
- Development environments and information should be on logically or physically separate hardware from production systems. Modifications to production systems must first undergo formal testing within a development environment.
- Any changes or modifications must follow the procedures outlined in the 'Information Technology Service Management' section of this policy.
- Prior to a new information system being developed or acquired the sponsoring School or Department management of the system must specify relevant information security requirements. Alternatives must be reviewed with the developers and/or vendors so that an appropriate balance is struck between information technology security and University objectives.
- Validation checks shall be incorporated into applications to detect any corruption of information through processing errors or deliberate action.
- Requirements for ensuring authenticity and protecting message integrity in applications shall be documented, and appropriate controls identified and implemented.
- Data output from an application shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.

5.3 Information Systems

5.3.1 The Chief Information Officer or delegate will manage:

- Information security responsibilities and ensure staff members are aware of their information security responsibilities.
- The privacy of individuals‟ information stored on information systems, as required under any applicable legislation.
- „Acceptable Use of Information Systems‟ section of this policy is maintained, outlining the responsibilities for individuals using University information systems & computing facilities.

5.3.2 The Chief Information Officer or delegate is responsible for maintaining:

- Contact with authorities for the investigation of and prosecution relating to information security breaches.
- A register of identified information security risks, including the following information as a minimum:
  - Asset Name / Identifier
  - Detailed risk description
  - Identified threats
  - Potential mitigating action(s)
- Contact with special interest groups to ensure the ongoing identification of localised threats and vulnerabilities.
- A register of all information technology assets for the purpose of identification, audit and investigation.
- Appropriate access controls and authentication mechanisms are in place to ensure information is only accessible by authorised individuals and systems.
- The „Information Systems Protection‟ sections of this policy (and where appropriate sub-sections), outlining the controls required to protect University information systems.
- An appropriate information security awareness programme is in place to ensure the ongoing education of information security responsibilities to all individuals with access to University information systems.
- Appropriate plans, procedures, documentation and arrangements to ensure the recoverability of information systems in the case of a disaster or major incident.

- University information should, where possible, be stored on centralised information systems. Information held on individual desktop computers or portable computers such as laptops should only be on a temporary basis.
- Passwords must not be shared with any other individuals unless the password is intended to be used for group purposes.
- Passwords must be managed following best-practice security guidelines.
- Prior to being released to third parties, all documentation that describes University system procedures, operations and processes must be reviewed by the Head Infrastructure and Contracts to ensure confidential information or intellectual property is not being inadvertently disclosed.
- Where permitted by the license agreement, all software must be copied prior to its initial use, and such copies must be stored in a safe and secure location. These master copies must not be used for ordinary business activities, but must be reserved for recovery from incidents.
- Unless specifically authorised by the Head Infrastructure and Contracts, individuals must not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate or compromise information security policy.

5.3.3 The Chief Information Officer or delegate will ensure that:

- Procedures are in place for the reporting and management of information security threats and vulnerabilities.
- Any updates or changes to Information Security or Information Technology Service Management related sections of this policy are communicated where appropriate throughout the University or to all policy stakeholders.

5.4 Information Systems Hardware

5.4.1 Information Services manages the total cost of the computing environment by aiming to reduce the total lifetime cost of ownership of these assets. This includes governance of the computer or device model selection, funding, selection of preferred suppliers; deployment, support, warranty and disposal. The strategy seeks to improve reliability and reduce the complexity of supporting computing devices, desktop and laptop computers.

5.4.2 The Standard Operating Environment supports hand held devices (mobile phones and PDA‟s), printers, Microsoft Windows and Apple operating systems which are described further in this policy.

5.4.3 All desktop and laptop computers are to be purchased in accordance with the University‟s Purchasing Policy.

5.4.4 The Information Services Capital Budget has allocated funds to cover some equipment replacement. This provides for end of life SOE desktop and laptop computer hardware models to be replaced on a one for one basis to the current specification from the established preferred supplier. New desktop or laptop purchases or upgrades to desktop or laptops will, in the first instance be funded through the School or Departments" annual operating budget and the account code will be provided at the time of making the purchase. Subsequent replacements will be funded through the Information Services Capital Budget for those machines held on the Computer Replacement list maintained by Information Services.

5.4.5 Purchases of additional new, or non-replacement SOE computers (i.e.: those that do not involve a corresponding transaction involving the return of a computer Glasgow Caledonian already owns or leases and which has an asset number attached to it) will be funded from School and Department operating budgets.

5.4.6 It is recognised that some areas may have specialist technical requirements to run applications that require computer hardware with specifications above that of the models prescribed. Areas wishing to purchase this equipment must complete a business case prior to purchasing for approval by the Chief Information Officer. In the event that the business case is successful the device will be supported by Information Services.

Computer hardware is inclusive of the components listed below with all other peripheral devices to be 100% funded from School and Department operating budgets:

- Desktop – computer, monitor, mouse, keyboard and installation cost;
- Laptop – laptop, port replicator, stand, mouse, keyboard and installation cost

5.4.7 The timing of replacement of desktop and laptop computers is based upon the economical life of the machines and best practise according to industry research. The end of life timescale for computing devices is five years.

5.4.8 University Laptops / portable computers must be locked away at night or properly secured.

5.4.9 External disk drives and other portable devices containing University information should be locked away when unattended.

5.4.10 Office doors must be closed and locked when the staff member is not present. This is of particular importance in public areas.

5.4.11 Data centres must be locked at all times and access should be on a need basis only. Rooms and cupboards containing cabling and network devices must be locked at all times and access should be on a need basis only.

5.4.12 Computers must not be removed or replaced when the owner of that machine is not present, unless prior permission has been obtained to do so.

5.4.13 All information must be removed from computer, external disk drives and other portable devices prior to disposal ensuring that all information is irrevocably erased.

5.4.14 Equipment or hardware normally stored within a computing facility must not be removed without prior authorisation.

5.4.15 The Head of Facilities Management must ensure fire detection/suppression, power conditioning, air conditioning, and other computing environment protection systems necessary to assure continued service for critical University information systems are provided and maintained.

5.5 Information Systems Protection

5.5.1 The Chief Information Officer or delegate will ensure appropriate backup procedures are established for recovery purposes. These procedures must meet or exceed any requirements set by the Internal and External Auditors.

5.5.2 Information stored on data centre systems must be backed up for recovery purposes.

5.5.3 Information backed up for recovery purposes should not be stored on the campus from which it originates. Backup information should be stored off-site, preferably replicated to another site well away from the campus.

5.5.4 To protect the University‟s information and ensure business continuity it is essential that the University has an effective anti-malicious software management system. The system should:

- Minimize the risk of malicious software throughout the University.
- Have a central management function.
- Enable automated configuration and transparently provide:
  - Automated updates of anti-malware software data files.
  - Upgrading of system version(s).
  - Downloading of new updates when required.

5.5.5 The Chief Information Officer or delegate shall ensure systems are provided and maintained to:

- Monitor for errors, performance problems and any abnormal activity or pattern of events
- Monitor the activity of systems administrators
- Detect unauthorised activity
- Monitoring systems should not record passwords or other authentication information that may be used to escalate privileges.
- To ensure the reliability of activity and event logs when monitoring and recording system information it is essential that all systems on the University networks include a time field that corresponds with the correct Greenwich Mean Time at the time of the event.

5.5.6 All University information systems must utilise secure authentication methods to ensure the confidentiality of passwords, codes and keys.

5.5.7 Sessions established with information systems must have appropriate timeouts and security measures to ensure unattended systems cannot be accessed by unauthorised individuals.

5.5.8 Access to administrative tools and security control systems are restricted.

5.5.9 Unauthorised access and breaches may result in disciplinary action.

5.5.10 Entry screens should display a warning message regarding the following information:

Use of this computer (which is monitored remotely) is subject to the conditions of Glasgow Caledonian University's Policies including the Information Policy and the University Regulations Pertaining To The Use of IT Equipment which are within this policy dated December 2011. When you click OK to this message you are agreeing to abide by these conditions which are found at http://www.gcal.ac.uk/staff/it/policies/

5.5.11 Appropriate measures to ensure hardware availability must be in place as described in the „Information Systems Hardware" section of this policy.

5.6 Information Technology Service Management

5.6.1 The Chief Information Officer or delegate will ensure the IT Helpdesk is available to function as a single point of contact for incidents and enquiries.

5.6.2 Procedures for the recording, categorisation, investigation and ongoing management of incidents will be established, maintained and monitored.

5.6.3 Process, procedures and measures to ensure the identification of underlying cause will be established, maintained and monitored for the purposes of problem management.

5.6.4 A knowledge base of known errors will be established, maintained and monitored, including any appropriate work-around information.

5.6.5 A centralised database of Configuration Items (CI"s) will be established and maintained to ensure an accurate view of all controlled assets.

5.6.6 Process, procedures and measures to effectively manage change to CIs will be established, maintained and monitored.

5.6.7 A repository of standard changes will be developed to assist with the system change management process.

5.6.8 A Change Manager will be responsible for the management and communication of changes to CIs.

5.6.9 The Chief Information Officer or delegate will ensure a change advisory board is established and operated to ensure adequate visibility of change.

5.6.10 Process, procedures and measures to control the distribution and implementation of new software and hardware releases will be established, maintained and monitored.

5.6.11 Appropriate environments for the building and testing of releases shall be developed.

5.6.12 All releases shall adhere to the system change management process.

5.7 Review

The Information Policy will be reviewed regularly by the Chief Information Officer to ensure it remains compliant with relevant legislation.

APPENDIX 1

UNIVERSITY REGULATIONS PERTAINING TO THE USE OF INFORMATION TECHNOLOGY FACILITIES

1. The Legal Framework

1.1 The use of IT facilities is subject to provisions of the following acts:

1.1.1 Data Protection Act, 1998

1.1.2 Telecommunications Act, 1984

1.1.3 Copyright, Designs and Patents Act, 1988 and subsequent regulations

1.1.4 Computer Misuse Act, 1990

1.1.5 Computer Copyright Software Amendment Act 1985

1.1.6 Criminal Justice and Public Order Act 1994

1.1.7 Race Relations Act 1976

1.1.8 Human Rights Act 1998

1.1.9 Regulation of Investigatory Powers Act 2000

1.1.10 The university draws to the attention of all users the University's statutory obligation under the Counter –Terrorism and Security Act (2015) to have due regard to the need to prevent people being drawn into terrorism.

1.2 Users must comply with the Acceptable Use Policy of the Joint Academic Network (JANET), a copy of which can be viewed at URL: **http://www.ja.net/services/publications/policy/aup.html**

1.3 Users must comply with any regulations and instructions displayed alongside IT facilities.

1.4 This policy is also relevant to and mentioned in the Revised Code of Student Discipline.

1.5 The University Information/records Management policy is also relevant in relation to the storage and retention of University Information.

APPENDIX 2

BEST PRACTICE GUIDELINES FOR THE USE OF GCU APPLICATIONS INCLUDING E-MAIL, FORUMS, BLOGS, WIKIS AND ALL OTHER ELECTRONIC MEANS OF COMMUNICATION PROVIDED BY GCU

Electronic forms of communication are often perceived as being closer to informal speech than formal writing. They can be sent quickly and often with little thought regarding their contents. What the sender may construe as acceptable could be construed as rude and abrupt by the recipient.

Therefore, the following best practice guidelines should apply when communicating via any electronic media:

- "GCU All" e-mails should not be sent other than in accordance with the internal communications policy administered by Communications and Public Affairs.
- Never say anything in an electronic communication that you wouldn"t say face to face. Electronic correspondence should not be used as a replacement to communicating with another member of staff in person.
- The inappropriate use of upper case in communications can be interpreted as undue emphasis and should be avoided.
- Messages should be concise and to the point. Staff/Students should not send heated messages (often called "flames") impulsively or in anger due to the impersonal nature of, for example, an email. It is far easier to harass someone this way than through face to face communication.
- Proof read content before sending to avoid misunderstanding.
- If the content of an electronic communication upsets you, do not reply back immediately; consult others, take time to think about the best action to take – e-mail, or any other form of reactionary response, may just make the situation worse.
- Check distribution lists or potential audiences before sending an e-mail and target recipients according to how important the message is to them
- The use of e-mail carbon copy (cc) or blind carbon copy (bcc) should be sparing and appropriate, for example it is best not to use this to embarrass or harass other employees.

Defamation/Libel/Slander

- Staff/Students must not write, send, publish, copy, distribute or forward derogatory or defamatory / libellous / slanderous remarks about any person or organisation (including the University) either on the Internet or by e-mail or any other Information system. If a member of staff discovers potentially defamatory / libellous / slanderous material, then they should report it to their line manager immediately. If a student discovers potential defamatory / libellous / slanderous material they should report it to their

Programme Organiser or Head of Division. Staff/Students must not send or forward discriminatory messages, even if it is intended as a joke, as this could be regarded as harassment. Staff/Students should be aware that anonymity of the internet is rare and most activity can be tracked to its source.

APPENDIX 3

GUIDELINES FOR THE REASONABLE USE OF INFORMATION TECHNOLOGY AND INFRASTRUCTURE

These guidelines are intended as a helpful aide memoire and staff and students should familiarise themselves with all relevant sections of the policy. The guidelines do not over-ride the policy requirements or restrict them by not comprehensively covering all aspects of the policy.

1. This instruction relates to all Information Technology and Network Infrastructure equipment, both mobile and static and accompanies the Information Systems Policy.

2. The term „Reasonable Use" means that all equipment will not be physically abused, excessively used for non work related purposes and the terms of use within the Information Systems Policy are to be adhered to.

3. On discovery of a fault or anomaly the member of staff or student is to contact the IT Helpdesk on extension 1234. This is applicable for ALL incidents. Examples of which are:

   3.1 Technical fault.
   3.2 Illicit e-mail, such as threats, pornography, bank detail requests, paedophilia, password requests, requests for credit card details etc.

4. It is important that when receipt of an inappropriate e-mail is detected, the offending e-mail must not be forwarded on to colleagues. Contact the IT Helpdesk on the above number and follow the instructions given.

5. Users should not divulge their user ID"s or passwords to others.

6. Static I.T. equipment is not to be moved from its location without authority.

7. Only one piece of I.T. equipment is to be connected to any one network socket.

8. Network extension leads/sockets connecting multiple I.T. devices to a single network point is not permitted.

9. All users should be aware that the IT Helpdesk will not e-mail any member of staff or student asking them for their log on details. It is important that such e-mails are not answered. Hackers and spam generators crop e-mail addresses from the Internet and send such e-mails to those addresses. A response indicates that the e-mail address is active and those are the ones that they concentrate on. This allows them not only to spoof (hijack) your e-mail address, but also gives them a way in to our network.

10. Users should also be aware that Banks will not ask you for account number, mother maiden name, your first school, date of birth, place of birth or any such similar personal data in a single e-mail, or by e-mail at all. Such e-mails should be reported to the IT Helpdesk on the above number. Users are strongly advised not to answer such e-mails.

11. When compiling your password to log on to our systems, do not inform anyone what your password is. This is your information and should be treated in exactly the same way as your PIN for your banks auto teller.

12. If your password is compromised, change it immediately.

13. Do not allow others to log on to our systems using your log on details. If this occurs and something was to go wrong, the system logs would show that you were the individual logged on at the time. You could therefore be held accountable for another"s actions.

14. E-mail should be archived on a regular basis. If this does not occur, Outlook will gradually take longer to load. If you are unsure how to archive e-mail, contact the IT Helpdesk on the above number.

15. Users are permitted to store data on H/Z drives. These are drives that are located centrally within the server rooms. Data on these drives are backed up to tape and stored off site. Users should endeavour to use such drives over the local drives on their workstations.

16. Users are reminded that the storage of holiday pictures, holiday videos, music etc. should not be stored on central servers. This uses data space and increases the length of time to complete backups while adding to the cost.

17. Mobile devices should be cared for in the same way as personal property.

18. Tariffs and the provider of our mobile devices have been negotiated by the university. Users should not change the SIM card, insert another providers SIM card or alter the mobile device in any way.

19. Workstations are not to be moved without notifying the IT Helpdesk.

20. Prior to transferring data from a mobile storage device to university computer, the data file should be subjected to an anti virus check. Once satisfactorily completed, the data may be downloaded.

21. Be aware that access to the internet is monitored. The viewing of inappropriate material is not permitted. In judging inappropriate material it is best to avoid any sort of images or media that would be classified as unlawful or 18 or R18 by the British Board of Film Classification (see classification guidelines at www.bbfc.co.uk).

22. Users should be aware that our systems are constantly monitored for inappropriate use. Users accept this by clicking „OK" of the log on dialogue box.

23. Use of university systems and internet connectivity is remarkably safe provided a few simple rules are adhered to. These are:

    23.1 Do not divulge your log on or password to anyone.
    23.2 Do not allow anyone to log on with your log on details.
    23.3 Do not divulge your log on or password to any request by e-mail.
    23.4 Do not divulge your bank, credit card or any personal details to any request by e-mail.
    23.5 Do not view inappropriate materiel on the Internet.
    23.6 Do not copy or store copyright materiel on your local machine or on central servers.
    23.7 Do not attempt to connect more than one device to a single network point.
    23.8 Be aware of those around you when viewing material on the Internet. What you find innocent, others may find grossly offensive.
    23.9 Be aware that all systems and the network are monitored for inappropriate use.
    23.10 Excessive use for non-work related purposes should not be undertaken.

24. University systems and supporting infrastructure are expensive. Both to procure and operate. These are done for the benefit of all staff and students. At times the university has been the subject of denial of service attacks, hundreds of spoofed e-mail being sent all over the world, credit card and bank details being compromised. The cost of each of these events is more than money, although that is significant. The cost also includes the stress for the individuals involved and risk to the reputation of our university. The annoyance factor is that each case was avoidable. Be careful with your log on and data!