

# **Kingston University** London

## **ICT Security & Usage Policy**

<b>Contents</b>	<b>PAGE</b>
1. Definitions	2
2. Audience	4
3. Introduction	5
4. Relevant Laws and regulations	7
5. Management Issues	8
Appendix A: Acceptable Use Policy for the ICT Users	10
Appendix B: Acceptable Use Policy for the Service Providers	17
Appendix C: Acceptable Use Policy for Email	23
Appendix D: Acceptable Use Policy for Mobile Devices	25
Appendix E: Acceptable Use Policy for the Halls of Residence Network Service	27
Appendix F: Acceptable Use Policy for the KU Presence Awareness Communication Service (PACS)	29
Appendix G: Acceptable Use Policy for the Use of Social Networking Sites	31

## **1. Definitions**

Where the terms “Kingston University”, “University” or “KU” are used, they will refer to Kingston University, River House, 53-57 High Street, Kingston upon Thames, Surrey, KT1 1LQ and associated locations.

The term “ICT” refers to any communication device or application, encompassing: radio, television, cellular phones, computer and network hardware and software, satellite systems and so on, as well as the various services and applications associated with them, such as videoconferencing and distance learning.

The term “user” refers to any person who accesses an ICT system, service or equipment owned, managed or supplied by KU or one of its partners.

The term “visitor” refers to any person who accesses an ICT system, service or equipment owned, managed or supplied by KU or one of its partners, but is not a KU student or KU member of staff.

“Partners” of KU refers to Kingston University Students Union and KUSCO only. In the context of this policy, it does not refer to our academic collaborative partners eg. St. George’s, Kingston College.

“Collaborative Partners” or “CP” refers to those institutions with which Kingston University has a collaborative arrangement in place for delivering courses.

“Infrastructure Security Manager” refers to the person responsible for all security, physical, systems and theoretical in relation to Kingston University and its partners.

The term “Production Systems Environment” refers to the physical areas where production systems reside such as Comms Room 1 or any faculty based server room.

“Manager of Facility” refers to the person(s) responsible for an area where ICT equipment may reside.

The term “network” refers to any data communications links such as Ethernet, fibre, or twisted pair etc that reside on KU sites or one of its partners or any connections between these sites or its partners.

“Shared Account” refers to a physical KU ICT account that is used by multiple persons.

The term “System Support Staff” refers to all helpdesk staff both Information Services and faculty based.

“filing systems” refers to areas where electronic data is stored.

“HORNS” refers to the KU halls of residence network service. Data communication points that are provided to students in KU halls of residence: Clayhill, Middle Mill, Seething Wells, Kingston Bridge House, Kingston Hill.

The term “Production Systems” refer to ICT systems that are used on a daily basis by users at KU. These systems are supported by Information Services or Faculty IT staff.

## 2. Audience

This document is for all users & providers of ICT equipment and services within Kingston University and all associated parties including those staff and students at Collaborative Partner institutions who have access to KU systems and services.

Acceptable Use Policy for the ICT Users & Acceptable Use Policy for Email applies to all that use ICT equipment and services.

Acceptable Use Policy for the Service Providers applies to all that provide ICT equipment and services to the user community.

Acceptable Use Policy for Mobile Devices applies to all users that carry out University business on a Mobile Device be it their own personal or University owned.

Acceptable Use Policy for the Halls of Residence Network Service applies to all users who have signed up for a data connection within their halls of residence room.

Acceptable Use Policy for the KU Presence Awareness Communication Service (PACS), also known as Instant Messaging, applies to all users in the KU community who have agreed to abide by the Acceptable Use Policy for ICT Users.

Acceptable Use Policy for the Use of Social Networking Sites applies to all KU Users who use Social Networking Sites.

### 3. Introduction

This ICT Security & Usage Policy forms a key part of the University's overall Information Security Policy. The ICT Security & Usage Policy focuses on the technical and usage issues in relation to the University's ICT systems whereas the Information Security Policy governs the broader issues of ensuring information is only read, heard, changed, broadcast and otherwise used by people who have the right to do so.

In using Information Communication Technology (ICT), users at KU have the ability to create, store and/or access a wide range of electronic information. The aim of the policy outlined in this document is to ensure that:

- The relevant information is always available to the relevant users.
- Confidentiality is always maintained.
- The integrity of the information is maintained.
- Data access and use conforms with regulations in regard to the Data Protection Act.

This policy is to enforce the appropriate use of ICT within KU and is reinforced by recommendations from JISC & UKERNA in line with ISO27001. The UCISA Information Security Toolkit (March 2005), designed to encourage best practice, has also been used as a foundation for this document.

The University needs to be aware of ICT security as there is a range of undesirable consequences associated with breaches of ICT security which include but are not limited to:

- Systems being unavailable
- Bad publicity and embarrassment
- Fraud
- Illegal personal investigation
- Industrial espionage.

This Policy comprises the following sections::

1. **Definitions** – This section defines terms used within this policy document.
2. **Audience** – This section states the audience to which this document applies.
3. **Introduction** – This section provides an overview of the policy.
4. **Relevant laws and regulations** – Covering the underpinning legislative framework.
5. **Management** – This section covers the management responsibilities such as incident handling, reviewing this policy and communication of this policy to users.

The following policies which support this document have been included here as appendices:

**Appendix A: Acceptable Use Policy (AUP) for ICT users** – This section sets out the framework for governing use of ICT systems and services by individuals of KU. This is the primary document that most users will need to read and accept.

**Appendix B: Acceptable Use Policy for ICT service providers** – This section sets out the security framework for the provision of Information Services that go beyond AUP for ICT

users section, in that it involves service provision rather than solely Information Services. This policy has a major impact on Information Services as the main provider of services but also impacts anyone providing services for others, e.g. Faculties, Educational Technology Unit.

**Appendix C: Acceptable Use Policy for Email** – This section sets out the framework for governing the use of the KU Email systems.

**Appendix D: Acceptable Use Policy for Mobile Devices** – This section sets out the security framework for using mobile devices for KU business.

**Appendix E: Acceptable Use Policy for Halls of Residence Network Service** – This section sets out the framework for governing the use of the KU network in halls of residence.

**Appendix F: Acceptable Use Policy for the KU Presence Awareness Communication Service (PACS)**

This section sets out the framework for the use of PACS, commonly known as Instant Messaging, within the University.

**Appendix G: Acceptable Use Policy for the Use of Social Networking Sites** – This section sets of the framework governing the use of social Networking.

This policy document will be updated and amended as required.

**This document has been approved by the following:**

<b>Group / Person</b>	<b>Date Approved</b>
University Information Committee	28 <sup>th</sup> June 2011
Senior Management Group	11 <sup>th</sup> July 2011

#### **4. Relevant Laws and regulations relating to this document**

It is the policy of the University that all of its activities must be conducted in accordance with current legislation. If a user of information is unsure as to their responsibilities in relation to the laws they should seek advice through their immediate supervisor.

The use of information is governed by a variety of different Acts of Parliament. These currently include but are not fully exclusive of:

- The Copyright, Designs and Patents Act 1988

- The Data Protection Act 1998

- The Human Rights Act 1998

- The Computer Misuse Act 1990

- The Regulation of Investigatory Powers Act 2000

- The Freedom of Information Act 2000

- The Electronic Communications Act 2000

- The Digital Economy Act 2010

- Together with various Statutory Instruments and other pieces of legislation.

In regards to dealing with breaches of this policy that are not criminal the appropriate University or partner organisation polices will be referred to. These include but are not limited to:

- Academic Misconduct – Undergraduate and Postgraduate Taught Courses

- Academic Misconduct – Research (Staff)

- Student Disciplinary Procedure

- Staff Handbook

- KUSCO Staff Disciplinary Procedure

## 5. Management Issues

In order for this policy to be employed effectively it is essential that those in a managerial position at Kingston University are personally fully aware of it and apply it in their own use of ICT.

Managers are responsible for:

- Ensuring that their staff, students and visitors only use ICT when they have agreed to follow the policy. This includes staff working in Collaborative Partner institutions who have access to University systems.
- For handling any disciplinary issues that arise and proactively investigating any suspected breaches.

Future students will be notified of the policy when they enrol. Future staff will be notified of the policy when they sign their contract of employment, or in the case of Collaborative Partners, when they complete the Data Collection template.

Visitors to KU will only be granted access to KU systems once they have signed to accept the policy.

The policy and any changes will be made available through StaffSpace and StudentSpace. Paper copies of the policy will also be available from the Information Services and Faculty Helpdesks.

### **Acceptance of this Policy**

All existing users of ICT will be notified of this policy and future changes. The users continued use of ICT after notification will constitute acceptance and agreement to the policy document.

### **Disciplinary Action**

Breaches of any sections of this policy are potentially disciplinary issues which will be handled by existing staff or student disciplinary procedures. Staff and Students must comply with the policy. Failure to do so may render them liable to disciplinary action which could, in serious cases, lead to dismissal from their employment or course.

### **Security Breaches**

Any suspicion of breach of the policy must be reported to the Information Services Service Desk immediately. Failure to do so constitutes a breach of this policy. There may be some instances e.g. sensitivities, users then may report a suspected breach to their line manager. The line manager then must report the issue to the Information Services Service Desk or direct to the Infrastructure Security Manager.

Within the current KU guidelines the Infrastructure Security Manager has the power to authorise ICT support staff to suspend access to all accounts affected by the breach. This may include accounts controlled by other departments. The Infrastructure Security Manager has the authority to suspend these accounts as well. Suspensions will be lifted in three working days unless further suspension is authorised by the Vice Chancellor.

In cases where investigation of traffic or content of user accounts is necessary then Information Services technical staff will carry out such work under direct instruction from the Infrastructure Security Manager following authorisation from the Director of Information Services or Human Resources Director (Staff) or Director of Student Administration (Students) and the University Secretary. KU will involve the Police in all cases where they believe illegal activity may have taken place.

#### **Updates and Amendments**

Information Services will ensure this policy is reviewed annually to reflect best practice with revisions being approved by the Vice Chancellor.

## **APPENDIX A**

### **Acceptable Use Policy for ICT Users**

This AUP forms part of the University regulations. The University is committed to maintaining standards. All users of ICT facilities must conform to Health and Safety requirements. The University reserves the right to investigate computer activity that is suspected to be detrimental to any persons, service or network or to be in breach of the AUP herein.

#### **1 Scope**

1.1 This policy applies to users of all KU central and departmental ICT facilities (including software) owned, leased or hired by the University, all users of ICT facilities on KU premises and all users of any ICT facilities connected to the KU networks.

#### **2 The Legal Framework**

2.1 Use of the ICT facilities is subject (inter alia) to the provisions of the following Acts:

2.1.1 Data Protection Act 1998

2.1.2 Copyright Designs and Patents Act 1988

2.1.3 Computer Misuse Act 1990

2.1.4 Freedom of Information Act 2000

2.1.5 Regulation of Investigatory Powers Act 2000

2.1.6 Electronic Communications Act 2000

2.1.7 Digital Economy Act 2010

2.1.8 Human Rights Act 1998

2.1.9 And any regulations made pursuant to these Acts.

2.2 Offences might be reported to the Police for further investigation and possible prosecution. Full details of the legislation are available from the Library.

### **3 Authorisation**

3.1 Use of any ICT facility is open only to staff, KU Partners and enrolled students of KU and any other persons authorised by the Manager of the facility (e.g. including visiting lecturers).

### **4 Registration**

4.1 Use of the facilities is conditional upon prior registration and the granting of a Username and an individual password. Such registration is carried out by Information Services for centrally-provided services, and by Faculty Technical Staff for Faculty based services.

### **5 Access**

5.1 On-Site ICT facilities will be accessible during published opening hours, or in certain circumstances by special arrangements. Remote access to some facilities is available 24/7 with best endeavours. Access will be contingent on system maintenance requirements.

### **6 Conditions of use for Hardware and Software**

6.1 Users must not in any way cause any form of damage to the University's computing equipment or software, nor to any of the rooms and their facilities and services which contain that equipment or software; nor to any of the network wiring infrastructure or communications equipment. The term "damage" includes modifications to hardware, software or infrastructure which, whether or not causing harm to the hardware or software, incur time and/or cost in restoring the system to its original state. All costs associated with repairing or replacing damaged equipment or software and/or in providing temporary replacements will be charged to the person or persons causing the damage. The costs will be determined by the University.

6.2 Users must comply with the terms and conditions of all licence agreements, available from the Managers of the ICT facilities, relating to any part of those facilities including software, equipment, services, documentation or other goods.

6.3 Users must not modify any software, nor incorporate parts of any software into their own work, without written permission from the copyright/intellectual property owner and the Manager of the ICT facility.

6.4 Users must comply with any instructions or regulations displayed in and around computing facilities.

6.5 Users must not introduce any virus, worm, malware, trojan horse or any other "nuisance" program or file onto any system or take any action to circumvent or modify any precautions taken by the University to prevent "infection" of its machines.

6.6 Users must not use the ICT facilities for sending any message textual or graphic or voice or video that is offensive, abusive, obscene, defamatory, racist or otherwise unlawful. Users must not initiate or spread electronic chain mail. Any electronic mail must be relevant to the user's course of study or job within the University and it must be sent only to those users to whom it is relevant.

6.7 Users may only access their own files and files which they have been given express permission to access.

6.8 Users must not use another user's Username nor permit or allow another user to use his/her own Username.

6.9 Users must not allow any password associated with his/her Username to become known to another user. The user will be held responsible for any unlawful action carried out under his/her computer account unless there is evidence to prove otherwise.

6.10 Users must not make known any other passwords which may be supplied to them in order to enable access to subscribed electronic resources.

6.11 Users must not connect any equipment to the University wired network without prior authority from ICT facility manager.

6.12 Every user of network facilities shall comply with any rules published for use of the networks and/or any ICT systems to which he/she has access over those networks.

6.13 Users must terminate each session in accordance with published instructions.

6.14 Interference with or removal of printout which belongs to another person is not permitted. Uncollected printout will be disposed of.

6.15 Printing credit in a student account will not be refunded at any time during the year or at the end of the academic year. Continuing students will carry their printing credit to the following year. Students leaving the University will not be refunded.

## **7 Behaviour**

7.1 The creation, display, production, downloading, uploading and circulation of offensive material in any form or on any medium is forbidden.

7.2 Users must respect the rights of others and should conduct themselves in a quiet and orderly manner when using facilities.

7.3 No equipment should be moved from its designated place or be tampered with in any way.

## **8 Equipment Loans**

8.1 No equipment or software may be borrowed without permission from the Manager of the ICT facility or ICT Facility loans team where available..

8.2 Security are authorised to stop and question any person seen leaving KU premises with equipment or software.

## **9 Private and Commercial Use**

9.1 The use of any of the University's ICT facilities for commercial gain as well as for private work (unconnected with a student's course or study at the University or a member of staff's legitimate activities) or for work on behalf of others is not allowed unless prior agreement has been made with the Manager of the ICT facility in question and an appropriate charge for that use has been determined.

## **10 Use of JANET and the Internet**

Use must comply with the JANET Acceptable Use Policy (available from <http://www.ja.net/documents/publications/policy/aup.pdf>), as published by the United Kingdom Education and Research Networking Association (UKERNA), which states that:

10.1 Subject to the following paragraphs, JANET may be used for any legal activity that is in furtherance of the aims and policies of Kingston University.

The following constitutes Unacceptable Use of JANET

10.2 JANET may NOT be used for any of the following (10.2.1 to 10.2.7 inclusive):

10.2.1 Creation or transmission, or causing the transmission, of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.

10.2.2 Creation or transmission of material with the intent to cause annoyance, inconvenience or needless anxiety.

10.2.3 Creation or transmission of material with the intent to defraud.

10.2.4 Creation or transmission of defamatory material.

10.2.5 Creation or transmission of material such that this infringes the copyright of another person.

10.2.6 Deliberate Creation or transmission of unsolicited bulk or marketing material to users of networked facilities or services, save where that material is embedded within, or is otherwise part of, a service to which the user or their User Organisation has chosen to subscribe.

10.2.7 Deliberate unauthorised access to networked facilities or services.

10.2.8 Deliberate activities with any of the following characteristics:

- wasting staff effort or networked resources, including time on end systems accessible via JANET and the effort of staff involved in the support of those systems;
- Corrupting or destroying other users' data;

- Violating the privacy of other users;
- Disrupting the work of other users;
- denying service to other users (for example, by deliberate or reckless overloading of access links or of switching equipment)
- continuing to use an item of networking software or hardware after UKERNA has requested that use cease because it is causing disruption to the correct functioning of JANET;
- Other misuse of JANET or networked resources, such as the introduction of 'viruses'.

10.3 Where JANET is being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of JANET.

### **University Rules for using Janet and the Internet**

10.4 The JANET Acceptable Use Policy applies also to the internal University network.

10.5 Commercial use is prohibited. Commercial use refers to any activity connected or involving any trade, profession, vocation or business not being any part of any function or purpose of Kingston University whether carried on solely or jointly or severally and/or whether or not with a view to profit or benefit any person or personal body other than Kingston University.

10.6 Recreational student use is allowed but students have to release the workstations if needed for course-related work. Unreasonable or recreational use by staff is prohibited during working hours.

10.7 Anonymous Email or any type of anonymous electronic information must not be sent.

10.8 Offensive material must not be sought or knowingly received.

10.9 Network services (e.g. Ftp or Web servers) must not be set up without first being registered with Faculty Computing staff or with Information Services. The person setting up the service will be held responsible for the secure operation of that service.

10.10 The University's Information Security Policies should be read as part of the University's regulations (INSERT LINK).

## **11 Disclaimers**

11.1 The University accepts no responsibility for the malfunctioning of any equipment or software that results in the failure of security or integrity of any stored program or data.

11.2 Student files and access will be removed once the student is no longer on his/her course. Students are advised to make copies on removable media of any data that they store on University services if they wish to keep it beyond this time, as the University will not be liable for its non-retention.

11.3 A staff computer account will be disabled once the member of staff's contract has been terminated. The University will not be liable for the non-retention of the member of staff's files beyond this time.

## **12 Monitoring & Access of ICT Systems & User Accounts**

12.1 The University may at any time permit the inspection, monitoring, or disclosure of ICT Systems and Data;

### **12.1.1 When required by and consistent with English law**

The University evaluates all such requests against the precise provisions of the Freedom of Information Act, Data Protection Act, The Regulation of Investigatory Powers Act, and other laws concerning disclosure and privacy, or other applicable law.

### **12.1.2 Policy compliance**

At the written request of the Vice Chancellor, Director of Information Services or Human Resources Director (Staff) or Director of Student Services & Administration (Students) and the University Secretary, if there are reasonable grounds to believe that violations of University policies have taken place. Existing policies can be found at <http://www.kingston.ac.uk/aboutkingstonuniversity/howtheuniversityworks/policiesandregulations/>

## **12.2 The University reserves the right to monitor ICT Systems:**

- 12.2.1 For instance to carry out system management, problem resolution, maintenance and capacity planning, to correct problems or for similar reasons related to performance or availability of the system
- 12.2.2 To address security issues, including virus management and authorised surveillance, including tracking unauthorised access to a system
- 12.2.3 The University may access, with written authorisation of the Vice Chancellor Director of Information Services or Human Resources Director (Staff) or Director of Student Administration (Students) and the University Secretary, the content of user accounts;
- 12.2.4 To meet time-dependent, critical business or operational needs or to carry out records management responsibilities; e.g. to conduct business during a crisis if an employee is absent when information is required, or prolonged absence of an employee when information in the User's account is required. The User will generally be informed at the earliest opportunity if this form of access is necessary.

## **13 Disciplinary Procedures**

13.1 Failure to comply with these conditions of use for facilities may result in the following procedures being invoked:

13.1.1 Withdrawal (whether permanent or temporary) of access to University ICT facilities. Such withdrawal may be invoked immediately after suspected breach of ICT regulation(s) has occurred. Reinstatement of access to ICT facilities will be through normal disciplinary procedures.

13.1.2 Recommendation to proceed through the University's disciplinary processes including exclusion from the University (student) or termination of contract (staff).

13.1.3 Referral to the Police for possible prosecution. Where appropriate.

THE DATA PROTECTION ACT (1998) applies to all users of the University's computers who process personal data (information relating to a living person). Further information and guidance regarding the requirements of the Act may be obtained from the University's Data Protection Officer, based in the University Secretary's Department, or from the website of the Information Commissioner's Office: <http://www.ico.gov.uk>

## APPENDIX B

### Acceptable Use Policy for the Service Providers

#### 1 Scope of this Policy

This policy applies to any ICT equipment and services that are accessed by KU users. This includes servers (data, web, application, others), information on servers, and communications equipment. Within this document all such devices are referred to as “systems”. Most of these systems are operated by Information Services and Faculty ICT staff but this policy also applies to any member of KU operating such equipment, for example a web server for a research project or a faculty based web application.

The “Acceptable Use Policy for ICT Users” also applies to staff involved in an ICT provider role.

#### 2 Roles

Within this policy a number of roles are referred to as defined below:

**2.1 Service Owner** – These are staff with the final authority for any item of equipment, software or set of information. For example the Human Resources Director would be the owner of KU’s HR system.

**2.2 Process Owner** – These staff are responsible for the business process that the ICT service supports. For example the payroll process would be owned by the HR Head Of Reward & Hr Systems.

**2.3 Service Managers** – These are staff who have been delegated by the service owner to carry out system management functions. Members of Information Services often carry out this role on behalf of service owners.

**2.4 Development Staff** – These staff carry out work that involves changing ICT systems. They have a duty to ensure that work carried out complies with this policy. If appropriate they will implement automated security measures.

**2.5 IT Operations Manager** – This member of staff is responsible for the day to day running of the central university ICT operations, including managing the operational staff and environment.

**2.6 Operational Staff** – These staff carry out work to ensure the correct operation of ICT systems in accordance with this policy.

**2.7 User Managers** – These are managers of end users, normally Heads of Schools, Heads of Service and Corporate Departments and Support Directors, who have a key role in approving requests for their staff to be granted access to information systems.

**2.8 Infrastructure Security Manager** – This member of staff has responsibility for ensuring that this policy is enforced.

### **3 Registration of ICT Systems**

All systems that fall within the scope of this policy must be registered with the Infrastructure Security Manager and operated as agreed.

### **4 Secure Network Boundaries**

**4.1 Security Zones** – The network will be designed to create security zones to reduce the possibility of internal or external users gaining unauthorised access to systems. ICT systems with particularly high security vulnerabilities will be protected both from internal and external access. All other systems by default will be protected from external access.

**4.2 Remote Access Facilities** – All users can gain access to KU externally via their own internet service providers thus connecting to KU through its main firewalled external pipe.

**4.3 Remote Management Facilities** - In special cases where it is necessary for users to connect directly into KU externally e.g. Operational staff out of hours maintenance, this will only be allowed with the service owners' approval, and only once security measures have been taken to ensure a secure connection.

### **5 Management of the Production Systems Environment**

The logical; and physical operational environment requires particular thought as access to this environment normally circumvents conventional ICT security. User ID's & passwords used in this environment that provide privileged access to systems for system management and operational reasons must be managed as below.

**5.1 Privileged Account ID's** – These user ID's will normally be allocated to specific staff but will **NOT** be the same as the ID they used for their daily access. In some cases these privileged accounts are dictated by the system hence are used by more than one member of staff but this will be avoided wherever possible.

**5.2 Privileged Account Creation/Modification** – Accounts will only be created with the written authority of the Service owner or his/her deputy, in conjunction with the Infrastructure Security Manager.

**5.3 Access rights** – Account configuration will be carefully considered to allow access only to appropriate information on the system as agreed by the Service owner. If necessary a member of staff may be issued multiple user ID's so that the privileged ID is only used when desired by their role.

**5.4 Logging Usage** – For privileged accounts all activity must be logged and the logs made available to Infrastructure Security Manager on request.

**5.5 Account Deletion** – Privileged accounts will be removed immediately they are not required for either operational or staffing reasons.

**5.6 Passwords** – All the principles defined for the management of passwords apply but due to the importance of the privileged access rights of these staff the following additional points apply:

- 5.6.1 The passwords must be changed at least 4 times a year.
- 5.6.2 For shared passwords they must be changed immediately when any member of staff with access to the passwords leaves KU, changes role, or is subject to disciplinary action.
- 5.6.3 Whenever system admin passwords are changed copies must be logged with the relevant System Custodian and Service owner, as well as in the central Information Services Comms Room 1 safe.

**5.7 External Staff** – Access to live systems by external staff must be supervised by operational staff and only once agreed by the Head of Production & Support Services.

**5.8 Physical Environment** – Access to systems and system consoles can allow normal security measures to be circumvented. All environments where such equipment is located must be physically secure and access limited as defined by procedures.

## **6 Backup and Media Control**

All systems must be backed up to removable media and copies stored in a secure remote location.

**6.1 Fault Tolerant Equipment** – Critical information systems where 24/7 service is required, consideration must be given to deploying fault tolerant equipment such as redundant power supplies and 'RAID' disk configurations.

**6.2 Backup Frequency** – All data must be regularly backed up.

**6.3 Backup Media Storage** – The media must be stored in fire proof safe remote from the physical system that has been backed up.

## **7 Computer Viruses and Similar**

Definitive measures must be in place to protect against the introduction, spread or storage of such programmes. Some can be quite harmful, erasing data or causing your hard disk to require reformatting. A virus that replicates itself by resending itself as an e-mail attachment or as part of a network message is known as a worm. All ICT systems must be running adequate anti virus protection as defined.

## **8 Managing User Accounts**

The following must be followed in relation to the management of user accounts on all ICT equipment:

**8.1 User IDs** – Where a service is provided to more than one department the standard KU ID should be used as issued by Information Services.

**8.1.1 Staff** the format is KU followed by the staff member's five digit payroll number; e.g KU13579

**8.1.2 Student** the format is K followed by the student's six or seven digit SITS allocated number; e.g K0498732

**8.1.3 Visitor** the format for staff is KX followed by a five digit number generated by the registration system. For students the format is KT followed by a five digit number generated by the registration system.

**8.1.4 Partner** The format for partners is KP followed by a five digit number generated by the registration system.

**8.2 Account Creation/Modification** – Accounts will only be created within the guidelines agreed by the service owner.

**8.2.1 Staff** the account holder must have a valid HR issued payroll ID number.

**8.2.2 Students** the account holder must have a valid student ID number issued by Student Administration.

**8.2.3 Visitor** the creation of an account requires the minimum of Head of School/Director of Service signature. Each account will have an expiry date which may be extended following the above procedure.

**8.3 Access Rights** – All accounts will be configured to allow access only to information on the system as defined by the service owner in accordance with the users' role.

**8.4 Account Deletion** – Procedures must be in place to remove accounts when no longer required.

**8.4.1 Staff** the account will be disabled immediately the staff member leaves KU, on notification by HR. Full deletion will follow in 3 months unless otherwise requested by the relevant Head of School/Director of Service.

**8.4.2 Student** accounts will be disabled when they are no longer shown as current via SITS data feed. The accounts will be deleted in a bi-annual batch process.

**8.4.3 Visitor** accounts will be deleted at the expiry date or earlier if requested following the same approval procedure as for the account creation.

**8.5 Account Suspension** - Procedures must be in place to suspend accounts instantly upon request from either Director of Information Services, Human Resources Director, Director of Student Services and Administration or the Infrastructure Security Manager.

**8.5.1 Staff** the account will be suspended immediately the staff member breaches the ICT Security & Usage Policy, or for other reasons (such as long term sick leave) on direct notification from the Human Resources Director.

**8.5.2 Student** accounts will be suspended immediately the student breaches the ICT Security & Usage Policy, or for other reasons on

direct notification from the Director of Student Services and Administration.

**8.5.3 Visitor** accounts will be suspended immediately the visitor breaches the ICT Security & Usage Policy, becomes in debt to the University, or for other reasons on direct notification from the Director of Information Services.

## **9 Managing Shared Accounts**

Shared accounts are only allowed for special purposes on the written approval of the Infrastructure Security Manager when their functionality is suitably restricted. These accounts will instantly be disabled when deemed necessary by the Infrastructure Security Manager in conjunction with the service owner.

## **10 Anonymous and Guest Accounts**

All accounts must be password protected and be associated to at least one named user who takes responsibility for additional accounts. Thus anonymous and guest accounts must not exist on any system.

## **11 Managing User Passwords**

All accounts must have passwords, and they must be created adhering to the following principles.

**11.1 Structure of Passwords** – Passwords will be at least 6 characters long, and should be alphanumeric and contain at least one other character of another type. Their structure must be random. Recognisable passwords may be allowed where the user is forced to change it the first time they log in. The new password must follow the structure as stated.

**11.2 Initial Passwords** – All accounts are allocated a random password on creation. Registered students, based at KU, will receive these passwords when they first log into a university machine; students from external institutions will need to obtain their password via a recognised proxy. Passwords for new staff will be sent to their line manager in time for their first day.

**11.3 Password Changing by Users** – All users have secure ability to change their own passwords. Staff will be forced to change their core password every 3 months for staff, students as defined by faculty.

**11.4 Password Changing by System Support Staff** – Only the owner of the account can ask for their account password to be reset, except in the case of KX & KT accounts where the account authority can make this request. This usually occurs if they forget their password. System Support staff will change the password once ID has been verified. The user will be prompted to change the password on their first login with the new password.

**11.5 Not displayed** – Passwords should never be displayed on screens or on physical media such as paper or post-it notes.

**11.6 Inactivity** – Staff must lock their desktops or log out if they are leaving their machine unattended. Students must not leave a desktop unattended, they must log out.

**11.7 Incorrectly Entered Passwords** – All unsuccessful logins will be logged. After 3 incorrect attempts within a period of 15mins the account will be locked and the user will need to seek assistance from systems support staff. The account will only be enabled once user ID has been verified.

## **12 Data Protection Act**

All data relating to individuals must be stored in securely and managed and processed in accordance with the Data Protection Act. Details relating to the Data Protection Act 1998 may be obtained from the university Data Protection Officer.

## **13 Investigating Security Incidents**

At times it will be necessary for Information Services staff when authorised by the Deputy Vice Chancellor, Director of Information Services or Human Resources Director (Staff) or Director of Student Administration (Students) and the University Secretary, to carry out investigations on suspected security incidents and other situations.

## APPENDIX C

### Acceptable Use Policy for Email

#### 1 Scope of this Policy

This policy applies to all users of the KU Email system. Email is available to all users within the KU community who have agreed to abide by the Acceptable Use Policy for ICT Users.

#### 2 Responsible Use of Email

Users sending Email from any KU owned domain (e.g. [xxxxxx@kingston.ac.uk](mailto:xxxxxx@kingston.ac.uk) or [xxxxx@kcq.co.uk](mailto:xxxxx@kcq.co.uk) ), are seen as representatives of KU and as such should act in a responsible manner.

- The sending of abusive, offensive, defamatory, racial or sexual content within an Email is strictly prohibited.
- The sending of Email that could be considered libellous to an individual or organisation is strictly prohibited.

#### 3 Personal Use of Email

Users are permitted to use the KU Email systems for personal use providing they adhere to the following:

- Personal views are clearly stated as such.
- Purpose is not for financial gain to the user or other organisation.
- The use does not contravene Acceptable Use Policy for ICT users.
- All personal email must be stored in a folder clearly marked as personal.

#### 4 Email Security

Email is not a secure form of communication and as such users must realise that any information sent via Email may be seen by other persons. Users are responsible for ensuring they don't compromise Information Security.

- The confidentiality of Email cannot be assured and as such users should carry out a risk assessment before sending confidential or sensitive information via Email.
- Users must not intercept or access other users Email without proper grounds and authorisation, and in accordance with the law.

#### 5 Monitoring and Access to Email

The University may at any time permit the inspection, monitoring, or disclosure of Email content;

##### 5.1 When required by and consistent in law

The University does not automatically comply with all requests for disclosure, but evaluates all such requests against the precise provisions of the Freedom of Information Act, Data Protection Act, The Regulation of Investigatory Powers Act, and other laws concerning disclosure and privacy, or other applicable law.

## **5.2 Policy compliance**

At the written request of the Vice Chancellor Director of Information Services or Human Resources Director (Staff) or Director of Student Administration (Students) and the University Secretary if there are reasonable grounds to believe that violations of University policies have taken place.

## **5.3 The University reserves the right to monitor Email in order:**

- 5.3.1 To carry out system management, problem resolution, maintenance and capacity planning, to correct addressing problems or for similar reasons related to performance or availability of the system
- 5.3.2 To address security issues, including virus management and authorised surveillance, including tracking unauthorised access to a system
- 5.3.3 The University may access, with written authorisation of the Faculty Dean (or nominee), the Human Resources Director, Director of Information Services or Deputy Vice Chancellor, the content of Email;
- 5.3.4 To meet time-dependent, critical business or operational needs or to carry out records management responsibilities; e.g. to conduct business during; a crisis if an employee is absent when information is required a prolonged absence of an employee when information in the User's Email is required. The User will generally be informed at the earliest opportunity if this form of access is necessary.

## **6 SPAM**

SPAM is defined as bulk Email communications that are unsolicited and not authorised by the KU executive. For example an invitation to a personal birthday party sent to the entire KU user community would be considered SPAM.

- 6.1 Users are strictly prohibited from the sending of SPAM within the University domain.
- 6.2 Users are also strictly prohibited from sending SPAM from the University domain to any other domain worldwide.

## **7 Attachments**

Network bandwidth is a valuable commodity to the University and as such users must be responsible when sending Email attachments.

Attachment limits for Email have been set at 15MB. This is a restriction not a target.

- 7.1 Users must not send harmful or dangerous content as Email attachments such as virus or worms. The sending and forwarding of chain emails is also prohibited.
- 7.2 The sending of multimedia content such as video or music files must be considered carefully, as this can have a serious impact on network bandwidth.
- 7.3 The sending of some attachments is blocked on the Email system; these include Executable files, Javascript files and security certificate files. A full list is available from Information Services.

## APPENDIX D

### Acceptable Use Policy for Mobile Devices

#### 1 Scope of this Policy

This policy applies to all users of mobile devices that are used for University business. The mobile device is owned by the University the user must agree to this policy or return the portable to their line manager.

#### 2 Types Of Mobile Device Available

Examples of the mobile devices KU supplies to its users, as authorised by their line manager are:-

- Blackberrys
- Laptops
- Mobile Phones
- PDAs

KU supplied devices are authorised to be connected to the KU ICT Infrastructure. Mobile device users must comply with all applicable Acceptable User Policies as defined in the KU ICT Security Policy.

#### 3 Personal Use of KU Mobile Devices

Users are permitted to use KU Mobile Devices for personal use providing they adhere to the following:

- Any personal calls or data use are clearly declared to managers, at which point a charge maybe incurred.
- The purpose or use is not for financial or any other form of commercial gain to the user or other organisation.
- The use does not contravene the KU Acceptable Use Policy for ICT users.

#### 4 Physical Security

Mobile devices if left unattended should be secured. For the working environment Information Services will make available desk locking cables for mobile device users where appropriate.

**5.1 Vehicle storage** - Do not leave mobile devices in vehicles. However, if no alternative is available store in a locked boot out of sight. Vehicle storage must not be used over night or for long periods of time.

**5.2 Room Storage** – Do not leave mobile devices unattended in open rooms. When the portable device is not in use it must be stored securely out of sight.

#### 5 Data Security

Any University data that is stored locally on a mobile device must be encrypted using the procedures set out by Information Services. Users must log into the mobile device to use it. All laptops must have up to date Anti-Virus software installed.

KU data must **not** be stored on personal mobile devices as it is not possible to verify the security of said devices.

## **6 Device Abuse**

Mobile device users must comply with The KU Acceptable User Policy For ICT Users, and pay particular attention to sections 6.6 and 7.1, reproduced here as 7.1 and 7.2 respectively:-

- 7.1** Users must not use the ICT facilities for sending any message textual or graphic or voice or artistic that is offensive, abusive, obscene, defamatory, racist or otherwise unlawful. Users must not initiate or spread electronic chain mail. Any electronic mail must be relevant to the user's course of study or job within the University and it must be sent only to those users to whom it is relevant.
- 7.2** The creation, display, production, downloading, uploading and circulation of offensive material in any form or on any medium is forbidden.

## APPENDIX E

### Acceptable Use Policy for the Halls of Residence Network Service

#### 1 Scope of this Policy

This policy applies to all users that have a network connection within KU halls of residence. The "Acceptable Use Policy for ICT Users" also applies to users within the halls of residence.

#### 2 Misuse of the Service

Misuse of the HORNS is taken very seriously - actions that disrupt network facilities will be subject to disciplinary proceedings. These can result in the withdrawal HORNS, suspension (temporary or permanent) or both. Examples of misuse include but are not limited to:

- Distribution or 'advertising' of material, shared over the network, on which you do not hold the copyright. In addition, the downloading or distribution of illegal software, or material likely to cause offence, is expressly forbidden;
- Attempts to damage, corrupt or remove the information on another user's machine without their knowledge, or to compromise the security of another user's machine;
- Attempts to circumvent the firewall or otherwise compromise network security (e.g. by HTTP tunnelling);
- Any action which results in the impairment of network performance;
- Running a DHCP server is not allowed for operational reasons - any user found to be running one may have their connection withdrawn permanently;
- Connecting more than one device to your HORNS data point;
- Commercial use;

#### 3 Terms and Conditions of Connection

Connection is for a single computer only. You must not attempt to connect another user's computer in your room or connect more than one machine at once. If you change your computer during the year, you should contact the Information Services Service Desk so that that your connection details can be reset. You are expected to ensure your machine is in good order:

- Individuals are responsible for all use of their HORNS connection and must not let others use their connection.
- Network devices such as routers, wireless routers, switches and DHCP servers if incorrectly configured can cause network disruption, and as such these devices must not be connected to HORNS.
- Users must install the latest critical security updates for their operating system.
- Users must enable the "Internet Connection Firewall" for their Local Area Connection if using Windows XP.
- Users must install an anti-virus program on their PC/MAC if they do not already have one and keep it up to date with the latest virus definition files.
- If any viruses are found, users are required to disinfect their PC/MAC and remove them.

- Information Services reserves the right to refuse or terminate a connection at any time.
- Breaches of AUP for ICT Users, AUP for HORNS or UK law may result in the disconnection of your HORNS connection without a refund.
- Information Services may disconnect computers with badly configured or faulty network cards that might impact on the performance of the network.
- Any computer infected with a virus will be disconnected from the network until it has been disinfected and patched if required.
- Users are responsible for the use and configuration of any software on their computer.
- Users are responsible for the security of their own system. Information Services will not accept responsibility for any harm resulting from the use of the HORNS.
- The service is normally available 24 hours a day 7 days a week but is vulnerable during maintenance periods. If a fault occurs outside office hours (0900-1700 Monday to Friday excluding public and statutory KU holidays) it will not be looked at until the next working day.

You are advised to read the following documents that are applicable to all students (all users are expected to read these guidelines, and ignorance of their contents will not be taken into consideration if they are broken.) Copies of the documents can be found on StudentSpace and in the Library:

- JANET (Joint Academic NETWORK) Acceptable Use Policy
- AUP for ICT Users
- AUP for email

#### **4 Currently Prohibited Software**

Users are currently not permitted to use the following software on the HORNS:

- Download managers, such as GetRight
- Filesharing software, such as Kazaa, BitTorrent and DirectConnect
- HTTP tunnelling software
- Share scanning software, such as Sharescan, LANster

Users are discouraged from leaving the following software running when not at their computers:

- Instant messaging clients

## **APPENDIX F**

### **Acceptable Use Policy for the KU Presence Awareness Communication Service (PACS)**

#### **1 Scope of this Policy**

PACS (also known as Instant Messaging) is available to all users within the KU community who have agreed to abide by the Acceptable Use Policy for ICT Users. This policy applies to all users of the PACS.

#### **2 Responsible Use of PACS**

Users sending instant messages from the KU domain are seen as representatives of KU and as such should act in a responsible manner.

- The sending of abusive, offensive, defamatory, racial, libellous or sexual content within PACS is strictly prohibited.
- Harassment or bullying via PACS will not be tolerated and may lead to an HR disciplinary matter. For further information please refer to current HR policies & procedures.

#### **3 Personal Use of PACS**

Users are permitted to use the PACS for personal use providing they adhere to the following:

- Personal views are clearly stated as such.
- Purpose is not for financial gain to the user or other organisation.
- The use does not contravene Acceptable Use Policy for ICT users.

#### **4 PACS Security**

PACS is not a secure form of communication and as such users must realise that any information sent via PACS may be seen by other persons. Users are responsible for ensuring they don't compromise Security.

- The confidentiality of PACS cannot be assured and as such users should not send confidential or sensitive information via PACS.
- Passwords of any kind should not be included in any PACS transmissions.

#### **5 Monitoring and Access to PACS**

The University may at any time permit the inspection, monitoring, or disclosure of PACS content;

##### **5.3 When required by and consistent in law**

The University does not automatically comply with all requests for disclosure, but evaluates all such requests against the precise provisions of the Freedom of Information Act, Data Protection Act, The Regulation of Investigatory Powers Act, and other laws concerning disclosure and privacy, or other applicable law.

#### **5.4 Policy compliance**

At the written request of the Vice Chancellor Director of Information Services or Human Resources Director (Staff) or Director of Student Administration (Students) and the University Secretary if there are reasonable grounds to believe that violations of University policies have taken place.

**5.5** The University currently does not actively monitor PACS but reserves the right to monitor:

- 5.5.1 To carry out system management, problem resolution, maintenance and capacity planning, to correct addressing problems or for similar reasons related to performance or availability of the system
- 5.5.2 To address security issues, including virus management and authorised surveillance, including tracking unauthorised access to a system

#### **6 Spam over instant messaging (SPIM)**

SPIM is perpetuated by bots that harvest PACS screen names via the Internet and simulate a human user by sending spam to the screen names via an instant message. The SPIM typically contains a link to a Web site that the spimmer is trying to market.

- 6.3 Users are strictly prohibited from the sending of SPIM within the University domain.

## APPENDIX G

### Acceptable Use Policy for Use of Social Networking Sites

#### 1 Scope of this policy

The policy applies to all Social Networking site users who have a relationship with Kingston University, either as a member of Staff at KU or KU Partner, or as a Student at KU or a KU Partner. Social Networking sites include but are not limited to Facebook, Bebo, Myspace, YouTube and Twitter.

#### 2 Responsible use of Social Networking

Kingston University understands the popularity and benefits of Social Networking sites if used responsibly. Such sites allow for, and promote, general communication, online discussion and provide the ability to share information about yourself and others quickly and easily. In many respects this can be beneficial to students and staff both in personal and academic terms. By following a few simple guidelines Social Networking can be enjoyed by all, safely and productively.

#### 3 Guidelines for use of Social Networking

**3.1** Before signing up to any Social Networking site make sure you have read the terms and conditions for that site, along with their privacy policy. If there is anything you do not understand or are not happy with, do **not** sign up to the site.

**3.2** When signing up to a site use only your personal details and not anyone else's. When filling in your personal details remember that these will be visible to other users. Only enter the details that you are happy with being in the public domain. It is **not** recommend that you fill in local addresses, telephone numbers or full dates of birth.

**3.3** If you upload any pictures to your profile, license to use these pictures in many cases is transferred to the Social Networking site in question. This allows the site to use the photo how they want to, possibly in marketing and advertising.

**3.4** You must **not** post any statements or photos that could damage the reputation of you, your family or that of Kingston University and its Partners. You must **not** make offensive or derogatory remarks about students, members of staff or other individuals, and you must **not** post obscene or derogatory images.

**3.5** It is important to remember anything you post on Social Networking sites may be visible to anyone, anywhere, at anytime! It is important to be aware of the risks and take steps to protect yourself and your personal information. Posting personal information could potentially lead to unwanted attention and could even contribute to identity fraud. For your own benefit, you should not post details which you might find awkward later, for example something you would not want family members or a future employer to see.

**3.6** It is important not to use the same username and password you use for other systems, such as your Kingston University login.

#### **4 Monitoring**

- 4.1** Social Networking Site Administrators, KU Officials, Police and other agencies can and do monitor these sites from time to time. KU Users of these sites must keep in mind that they could face disciplinary action by breaching KU policies. They could also be subject to criminal proceedings if their actions are found to be illegal.
- 4.2** It is now common practice for employers to search Social Networking sites as a means for screening potential applicants for positions of employment.