Procedure: Student - Acceptable use of IT

Department: ITIS

Date: June 2015 V1.0 **Review Date: June 2016**

1.0 Purpose

This procedure defines what is acceptable and what is unacceptable when using the University's IT facilities as provided by the University or its partner providers. It also defines the responsibilities of all registered students in complying with it.

2.0 Scope

University IT facilities include:

- Internet access via Broadband or other service
- Physical cable fibre & copper around campus
- Computer & telephony networks wired & wireless
- Physical or virtual computers, whether servers, desktops, terminals or mobile devices
- Peripherals such as monitors, keyboards and printers
- IT Applications used on the University Network
- Software and data on University IT facilities
- Other computer-based information systems provided for any purpose e.g. CCTV, door access ("University IT facilities").

This procedure applies to all University IT facilities, whether they are located on University premises or Non-University premises and to all registered students of the University.

Note: Where more specific constraints on the use of University IT facilities have been specified by the University at any time, the more restrictive requirements must be observed.

3.0 Compliance and Non-Compliance Consequences

Compliance with this procedure is mandatory and non-compliance must be reported to the IT Helpdesk to record the incidence and escalate to the appropriate authority to determine the action to be taken.

Students must note that any breaches of this procedure may be treated as misconduct under the University's relevant disciplinary procedures and could lead to disciplinary action or other actions deemed appropriate to the circumstances, such as removal of access to University IT facilities and/or fines.

In the event of extreme cases affected by English Law, non-compliance may also be reported to the appropriate external authorities.

4.0 Procedure

4.1 Responsibilities

The Associate Director Service Operations is responsible for defining, reviewing and publishing this procedure and for providing guidance and advice in support of it.

Heads of Department and Directors are responsible for ensuring that all students within their area are made aware of the procedure and act in accordance with this procedure.

Each and every student is responsible for ensuring that their use of University IT facilities is acceptable and will be accountable for all actions undertaken using their University credentials (username and password).

4.2 Acceptable use

University IT facilities are provided to support students with their studies and for conducting University related pursuits. Reasonable personal use of University IT facilities by students (i.e. use not related to a student's studies or University-related activities) is permitted, provided this does not interfere, either by its timing or extent, with the availability of University IT facilities to other users for teaching, research or administrative purposes.

Further restrictions may be put in place in public areas at specific times, for example during registration or examination/revision periods.

The University provides internet access across campus including several Halls of Residence for the use of students for academic and social purposes in a responsible, reasonable & collaborative manner. Students are asked to recognise that capacities are finite and excessive use will detrimentally affect other users.

The University has no liability for any personal loss or damage suffered by a student through personal use of the University IT facilities, for example the theft of credit card data used online. The University does not provide any guarantees regarding the privacy or security of such personal use; for example, the University may require access to data in accordance with section 5 below.

4.3 Unacceptable use

All unlawful activity carried out, on, or through the use of University IT facilities is unacceptable: the police will be informed where there is any evidence of such activity.

In addition, Goldsmiths has a statutory duty, under the Counter Terrorism and Security Act 2015, termed "PREVENT". The purpose of this duty is to aid the process of preventing people being drawn into terrorism.

Unacceptable use of University IT facilities includes the following activities, some of which may be deemed unlawful in certain circumstances:

- Using IT facilities or social media to create, download, store, transmit, share or display any unlawful material, or material that is indecent, offensive, defamatory, or extremist.
- Using IT facilities or social media to harass, bully, threaten, defame, abuse and libel.
- Using IT facilities to unlawfully discriminate, or to encourage unlawful discrimination , on the grounds of age, disability, sex, gender reassignment, pregnancy, maternity, race (which includes colour, nationality and ethnic or national origins), sexual orientation, religion and belief or because someone is married or in a civil partnership.
- Activities with any of the following characteristics:
    - corrupting or destroying other users' data or violating their privacy through use of University IT facilities;
    - using the University IT facilities in a way that denies service to other users (for example overloading network capacity);
    - the introduction of malware (such as viruses) and/or password detecting software;
    - hacking activities;

- Disguising, or attempting to disguise, the identity of the sender/origin of an electronic communication; and/or using University IT facilities to misrepresent any views and/or opinions held personally by the user as the views and/or opinions of the University, unless the user is explicitly authorised to do so.
- Tampering with University IT facilities without written permission for example rebooting WIFI Access Points around campus.
- The transmission of spamming communications containing commercial or promotional material which do not make provision for recipients to opt-out of receiving such communications.
- Unauthorised disclosure of sensitive or confidential information obtained from, or disseminated through use of, University IT facilities
- Use of personal data, through use of the University IT facilities, in breach of the Data Protection Act 1998.
- Using University IT facilities to undertake actions which undermine the security controls or procedures which have been implemented to protect systems and data, for example, sharing passwords.
- Deliberately wasting staff time or IT resources.

- Using University IT facilities to create, download, use, transmit, share and/or display material, including software, which would result in copyright infringement. Students must ensure that they do not breach copyright laws and must not create, download, use, transmit, disseminate and/or display any material which is subject to copyright without the appropriate permission(s). Peer to peer sharing such as torrent will be blocked & subject to management consent having validated the legality of the application.
- The installation, and consequent use, of software on University IT facilities where such installation and use is not permitted by the University. If in doubt, students must speak to a member of IT services.
- The connection of IT equipment not owned, leased, hired or otherwise provided by the University (for example, the connection of portable or privately owned equipment), unless agreed in writing by the IT IS Management team. Any device attached without these permissions will be deemed “rogue” & may be blocked and investigated by the IT&IS.

4.4 Exceptions

- Where use of University IT facilities for what would be considered inappropriate use under this procedure is required for University-related activities (such as lawful research), the user must seek the prior written permission from IT&IS.

5 Monitoring compliance

No member of staff is permitted, as a matter of routine, to monitor an individual’s use of University IT facilities. However, where, for example, there are reasonable grounds to suspect an instance of inappropriate use, misuse or abuse of any University IT facilities, or where a legitimate request is made by the police or other authority, IT&IS may grant permission for the monitoring or investigation of a student’s use of University IT facilities. This could include any data traffic transacted through the university network including email and the internet (for example, use of social media websites).
Routine monitoring of inappropriate internet use is in place to ensure data traffic to and from the Janet network is appropriate. Traceability for this is provided by the University firewall.

6 Associated documents

Please refer to:
- Appropriate Use of IT Policy
- Staff – Appropriate Use of IT Procedure
- User – De-activation for inappropriate use procedure

7 Review of procedure

This procedure will be reviewed at least every two years or when there are significant changes to it.

8 Contact list for queries related to this procedure

Associate Director Operating Services
Chief Information Officer

9 Authority for this procedure

Chief Information Officer