Policy: Appropriate Use of IT

Department: **ITIS**

Date: **Approved October 2015** **Review Date:** **June 2016**

1.0 Purpose

This policy outlines the main principles of what is acceptable and what is unacceptable when using the University's IT facilities as provided by the University or its partner providers.

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 policy applies to all IT users (staff, student, visitor, contract etc.) of the University IT facilities, whether they are located on University premises or Non-University premises and to all registered students of the University.

3.0 Responsibility & Compliance

The Chief Information Officer is responsible for this Policy.

Heads of Department are responsible for ensuring that all staff and students within their area act in accordance with this policy and associated procedures.

The ITIS Department is responsible for providing policies, procedures, guidance and advice in support of this policy where required.

Each user of University IT facilities, whether they are a member of staff or a student, is responsible for ensuring that their use of University IT facilities is acceptable and is accountable for all actions undertaken using their University credentials (username and password).

Compliance with this policy 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.

3.1 Acceptable use

University IT facilities are provided to staff, students and authorised parties for University related activities.

Reasonable personal use is permitted as long as this does not have a detrimental effect on the availability or performance of IT facilities for other users.

The University provides no guarantees in regard to the privacy or safety of any personal use.

3.2 Unacceptable use

All unlawful activity carried out on or through the use of University IT facilities is unacceptable.

In addition, Goldsmith 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: using University IT facilities to conduct unlawful activity; bully or discriminate; hack and introduce malware (such as viruses); download, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening, discriminatory or extremist.

All users should refer to the following Standard Operating Procedures for further definition of unacceptable use of IT facilities:

- Staff – Appropriate Use of IT procedure
- Student – Appropriate Use of IT procedure

4.0 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, the Chief Information Officer or appointed Deputy may grant permission for the monitoring or investigation of an individual'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.

5.0 Associated documents

Please refer to:

- Staff – Appropriate Use of IT Procedure
- Student – Appropriate Use of IT Procedure
- User – De-activation for Inappropriate Use Procedure

6.0 Review of policy

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

7.0 Contact list for queries related to this policy

Chief Information Officer

8.0 Authority for this policy

Senior Management Team