Goldsmiths
UNIVERSITY OF LONDON

Procedure: User – De-activation for inappropriate use of IT

Department: **ITIS**

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

1.0 Purpose

This procedure defines process for the de-activation of users from access to University IT facilities who have contravened the Appropriate Use of IT Policy & associated procedures.

2.0 Scope

All users who have access to University IT facilities including:

- 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.

3.0 De-activation

In the event that any user is suspected of contravening the University Appropriate Use of IT Policy the following sanctions are recommended:

LEVEL 1 – Unlawful use

Where the user is suspected of breaking English Law their account will be suspended with immediate effect and reported to their line manager or Head of Department, and Associate Director Service Operations. All IT transaction records are to be retained pending the appropriate investigation and potential involvement of the Police.

LEVEL 2 – Inappropriate use impacting other users

Where the user is suspected of causing a nuisance through unacceptable practice e.g. resource hogging, malicious messaging, introducing malware/viruses etc. his or her account is to be suspended with immediate effect and reported to their line manager or Head of Department, and Associate Director Service Operations.

The suspension will remain on that users account until Associate Director Service Operations confirms that a suspension can be lifted following the appropriate investigation outcome.

LEVEL 3 – Inappropriate use risk

Where a user is suspected to be contravening the Appropriate Use of IT Policy either deliberately or inadvertently but this is unlikely to impact other users, the IT IS team will record the incident in the first instance. This should then be highlighted to the Associate Director Service Operations for urgent investigation prior to the suspension of the user account.

The Associate Director Service Operations will then determine the appropriate course of action which could include a period of monitoring, immediate suspension, reminder of the policy etc. depending on the level of risk associated.

Independent of the level of concern all data and records will be retained as they may be required as evidence should the incident escalate and require the attention of the appropriate authorities.

Upon the successful conclusion of investigation a user can be re-instated only with the written permission of the Associate Director Service Operations following sign off in the incident log.

4 Incident recording

All incidents of de-activation or the risk of de-activation should be recorded by the Associate Director Service Operations in the incident log and retained for a minimum period of seven (7) years.

5 Associated documents

Please refer to:

- Appropriate Use of IT Policy
- Student – Appropriate Use of IT Procedure
- Staff – Appropriate Use of IT Procedure

6 Review of procedure

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

7 Contact list for queries related to this procedure

Associate Director Operating Services
Chief Information Officer

8 Authority for this procedure

Chief Information Officer