APPENDIX C: IT USAGE POLICIES AND REGULATIONS

Purpose and scope

1. These Conditions of Computer Use are a formal statement of what is acceptable and unacceptable when using the College's IT facilities and network. They aim to encourage responsible behaviour and good practice, thus assisting the College in maintaining a secure, safe and robust IT environment.

2. The conditions detailed here apply to all users of the College's IT facilities whether members of staff, students, or people from outside the College who have been authorised to use facilities.

3. All users should be aware of these conditions and abide by them. Contravention could lead to loss of access to IT facilities and disciplinary action. If you are unsure about any aspect of these Conditions of Use or your use of College's IT facilities, you are responsible for seeking clarification by contacting the College's IT Helpdesk.

4. Information Services will make all users aware of these Conditions of Computer Use when they are issued an IT account. Reminders will also be communicated regularly. Each Faculty or Division and their constituent Departments is also responsible for ensuring that this document is brought to the attention of users within their domain during induction processes for new staff and students and at other times when appropriate.

5. This policy applies to all IT facilities owned by the College as well as those owned by third parties for which access has been facilitated by the College. It also applies to personally owned equipment used to access any of the College IT facilities.

Definitions

6. 'IT facilities' means all computing equipment such as servers, PCs, laptops, tablets, smartphones and printers; software, data and information held on those systems; information systems used for administrative and other purposes; network access via wired and wireless connections; online services; and the user credentials used to identify you and manage access to facilities.

7. In these regulations, 'device' means any equipment that can be connected to the College network including PCs, servers, laptops, as well as mobile devices such as phones and tablets.

8. In these regulations, 'computer' means PCs, desktop systems, servers, laptops and notebooks.

Summary of conditions

9. Your College password is confidential and you must never disclose it to others, or let anyone else access services and systems using your password. Disclosing your password to others contravenes the Conditions of Computer Use and could lead to disciplinary action and loss of access to IT facilities.

YOU SHOULD NOT RESPOND TO ANY REQUEST TO DISCLOSE YOUR PASSWORD INCLUDING THOSE SEEMING OR CLAIMING TO COME FROM THE COLLEGE OR INFORMATION SERVICES.

10. Be aware of relevant legislation. In particular, if you work with personal information about individuals, you must be aware of and comply with the Data Protection Act. You should also be aware that College computer communication systems depend on the Joint Academic Network (Janet) and all use must comply with Janet's Acceptable Use Policy.
11. Computing facilities are provided for College work purposes. Limited personal use is permitted, provided it is not illegal, does not adversely affect other users, does not interfere with work or studies, or does not in any other way breach the Conditions of Computer Use. Staff should not use the College email service for personal (non-work related) emails.
12. Care must be taken to ensure you do not create, transmit or publish any material that is illegal, offensive, abusive, or whose effect is to bring the College into disrepute.
13. Files are private. You must not try to access files or computer systems that you are not authorised to access.
14. Electronic media are subject to copyright. It is illegal to make an electronic copy (e.g. by scanning, downloading, copying from disk) unless you have the appropriate copyright authorisation.
15. Software is subject to copyright and licensing restrictions. Software provided by the College should only be used by members of the College for College purposes and in line with licence conditions of the software. You should not install, copy or distribute it to others unless authorised to do so.
16. Care must be taken when introducing software/data into the College. Only those using approved processes or authorised to do so should install data or software onto College-owned devices and they should ensure it has been

checked for viruses or other malware. Where necessary, administrative rights may be granted to permit users to install software on College devices.

17. Do not transmit files/data to others without first checking for viruses or other malware.
18. If you are responsible for supporting others and the systems and services they use, you have an additional responsibility to ensure that those systems and services are secure, and you should encourage good practice in those that use them. Ensure that computer systems in your care are secure against unauthorised access, have up-to-date operating systems and application software security patches applied, and (where feasible) have up-to-date anti-virus/anti-malware software installed.
19. All personally owned electronic devices connected to the network must be registered following processes described at http://www.gsmlondon.ac.uk/cts/itregs/equipreg
20. If a device has been registered using an authorised self-registration process (e.g. in student common rooms), the owner is responsible for security of that system and any activity on it. If inappropriate activity is detected arising from the device, the registered owner will be held responsible for it. The owner should ensure that the system has up-to-date operating system and application software security patches applied, and (where feasible) has up-to-date anti-virus/anti-malware software installed.
21. Use of College computer systems and the network is monitored. The College has the right to access files, intercept communications, or monitor usage if there are grounds for suspecting misuse. In cases of possibly illegal activity, copies of relevant information may be handed to the police.

Conditions of use

Access to College IT facilities

22. Use of the College's IT facilities is restricted to the following registered users, authenticating by means of a College IT account:
    (a) Students registered with the College for a study programme.
    (b) Staff holding a contract of employment with the College.
    (c) Other individuals who have been sponsored by the relevant Head of Department/Department, or their nominated deputy.

Access to specific IT facilities is authorised by the facility owner

23. Limited access to the College's IT facilities is available to users authenticating by other means such as Eduroam.

24. Further information on the above and the facilities and services they are entitled to use are detailed in the Information Services Directorate (ISD) User Entitlements Policy, which is available at https://www.gsmlondon.ac.uk/is/strategies/User-Entitlements- Policy.

Acceptable use

25. Computing facilities are provided for the pursuit of legitimate College activities:
    (a) Teaching and learning.
    (b) Research.
    (c) Personal educational development.
    (d) Administration and management of College business.
    (e) Any other lawful activity that furthers the College's mission.

26. Limited use of the College network and IT facilities for personal purposes other than College work or study, e.g. access to the internet, is permitted. However, such use must not interfere with work or studies, must be legal and must be strictly in line with the requirements in these Conditions of Computer Use.

Unacceptable use

27. All the following are expressly forbidden when using the College's network and IT facilities:
    (a) Any illegal purposes. The police will be informed where there is evidence of illegal activity.
    (b) Accessing, creating, storing or transmitting (other than for properly supervised and lawful purposes[1]) offensive, obscene or indecent data or images, or data from which such material could be derived, or material that may be subject to counter-terrorism legislation.[2]

NOTE: The College has a statutory duty, under the Counter Terrorism and Security Act 2015, termed 'Prevent', to aid the process of preventing people being drawn into terrorism.

[1] Lawful purposes include approved teaching or research, or an investigation by authorised personnel into suspected abuse of College facilities.

[2] Where academic use is likely to include such material, authorisation should first be sought from the Head of Department and the relevant research or ethics committee and the Information Services Assistant Director Strategy, Policy and Compliance made aware. . Consultation with external authorities may be required and is advisable under certain circumstances depending on the nature of the activity. . In particular, all use of material subject to counter-terrorism legislation must be used only in line with the Counter-Terrorism and Security Act 2015 and the guidance applying to Higher Education institutions in England and Wales. . Security sensitive material must be handled following UUK guidance http://www.universitiesuk.ac.uk/highereducation/Pages/OversightOfSecuritySensitiveResearchMaterial.aspx.

(c) Creation or transmission of material that is designed or likely to annoy, harass, bully, inconvenience or cause needless anxiety.

(d) Creation or transmission of material with the intent to defraud.

(e) Creation or transmission of defamatory, discriminatory or libellous material, or material whose effect is to bring the College into disrepute.

(f) Transmission (including downloading, uploading, and streaming) of material that infringes the copyright of another person.

(g) The unauthorised distribution to third parties of any information in which the College or partner organisations such as research funders have intellectual property rights.

(h) Unauthorised interception or hacking of communications over the network including e-mail and telephone messages.

(i) Transmission of unsolicited commercial or advertising material within the College or externally, unless authorised to do so on the College's behalf and where that material relates to a service to which the recipient has subscribed.

(j) Unauthorised access or trying to gain unauthorised access to IT facilities or services both within and outside the College.

(k) Disclosing your College password to others, or letting others use your College IT account, regardless of whether they are College members.

NOTE: Users are responsible for the security of their password. They should under no circumstances disclose it to others, whether in response to an email, by visiting a web page, in person, or over the telephone; nor should they allow others to use their IT account (including members of College or external parties). Failure to comply with this may result in loss of access to facilities or disciplinary action. If a user has previously been detected as having disclosed their password to others and after having been duly warned is discovered to have disclosed their password on a subsequent occasion, they will lose access to IT facilities. The matter will be reported to the appropriate College disciplinary authority for further action.

(l) Deliberate activities having or likely to have any of the following characteristics:

- Corrupting or destroying others users' data.
- Violating the privacy of others.
- Disrupting the work of others.
- Causing annoyance to others by inappropriate or inconsiderate use of computing facilities (e.g. internet phones in IT areas).
- Using applications for non-academic purposes that are likely to result in excessive network traffic causing disruption to others.

- Denying service to others.
- Continuing to use an item of software/hardware after Information Services has requested that such use cease.
- Other misuse of College IT facilities or resources, such as the introduction of malicious software, in such a way that it compromises the security of College systems and the network.

(m) If the College network is being used to access another network, any deliberate or persistent breach of the acceptable use policy of that network.

NOTE: If an individual is absent from work for a long period or leaves the College without first passing on their digital assets, and access to their IT account is needed to progress College business, then access to it by another authorised individual can be granted if authorised by the relevant Head of Department.
(When a member of staff leaves, their account is frozen, and deleted 100 days after their contract end date.)

Data protection and security

28. The College must keep certain personal data about staff and students to fulfil its objectives and meet legal obligations. The law requires that this data must be collected and used in a fair manner, be accurate and up to date, stored securely for no longer than needed to fulfil its stated purpose and not disclosed to any other person unlawfully.

(a) No user may use the College's computer systems to hold or process personal data except in line with the Data Protection Act (DPA) 1998.

(b) Staff must not construct or maintain computer or manual files of personal data unless required to do so as part of their work responsibilities and as approved by their manager.

(c) Students must not construct or maintain computer or manual files of personal data for use in academic studies or research without the express authority of an appropriate member of staff, normally their supervisor or Head of Department.

(d) Those in the College who have data in their care, or who are authorised by the College to process personal data, should ensure they are aware of their obligations under the Data Protection Act and comply with the Data Protection principles. These principles, along with more information about the Act and its applicability at the College, can be found at http://www.gsmlondon.ac.uk/is/strategies/infregs/dp. In particular, the removal of personal data from the College should be minimised. Encryption must be used when taking personal data off site by any means

including use of mobile devices, removable storage or emails to external email addresses to avoid the possibility of inadvertent and unintended disclosure to unauthorised third parties (the seventh data protection principle). Personal data must only be transmitted or transported in an encrypted form.

(e) If you share personal data with third parties external to the College, a data sharing agreement must be in place to govern the sharing. Contact the Data Protection Officer for advice (data.protection@gsmlondon.ac.uk).

(f) If you have data in your care about College research, teaching or administration, you should also be aware of and comply with the following:

- The College's General Information Security Policy – see http://www.gsmlondon.ac.uk/is/strategies/infregs/infosec/gisp.
- All data should be assessed on its strategic value and level of confidentiality. It should be stored and handled in line with policies and controls detailed in the Information Classification and Data Management Policy. See http://www.gsmlondon.ac.uk/is/strategies/infregs/Information+classification+policy.

(g) Managers of staff with data responsibilities must ensure their staff follow College security policies and advice, and in general adopt good practices in this regard.

(h) Users using devices configured to synchronise with or link to any College IT service (such as the Exchange server or filestore) must set security on the device to prevent unauthorised access. Staff using their own personally owned devices for conducting College business including receipt of emails should ensure that the devices and the data held on them are secured to the same standard as defined in the College's information security policies.

(i) Users should not root or jailbreak (i.e. circumvent the security) any College-owned devices. Devices operated in this state are liable to be more easily compromised. Any attempt to bypass the security built into a device is potentially an offence under the Computer Misuse Act 1990.

Copyright

29. Copyright material may only be copied if the copyright owner has granted permission, directly or through a licensing scheme. 'Copying' includes scanning,

recording, streaming, and downloading, and covers print, digital and web-based material.

30. Copyright material should not be networked or otherwise shared with multiple recipients without first getting the rights owner's permission or ensuring that such action is covered by an appropriate licence.

Software

31. Software is subject to copyright and licensing restrictions and people involved in illegally reproducing software may be subject to civil damages and criminal penalties.
32. Software provided by the College must only be used in line with licence conditions of the software. You must not copy or distribute it to others unless authorised to do so.
33. In general, all users are expected to honour any agreements or contracts made by the College concerning any computer software or data that they use and to abide by the general principles as detailed in the Software Copyright Acknowledgement document which is available at http://www.gsmlondon.ac.uk/is/itregs/softwarecopyright.
34. Software licence agreements vary. The principal user of a single-user system or the manager of a multi-user or networked system is responsible for the software loaded on that system and ensuring that it is used in line with the licence agreement.
35. Software provided by the College should not be installed, removed, disabled or altered, except by approved methods.
36. Users must co-operate with people employed by the College to carry out software and data audits, and where required follow software registration procedures.
37. Departments must keep an up-to-date inventory of all software installed on their computer systems. They must ensure that no software is installed for which the College lacks a current licence.
38. Departments must also ensure that any College-licensed software is returned by leaving members of staff or students and any copies are removed from computers within their care, before leaving the College.

Computer security

39. All access to computers and the network should be authenticated by a username and password.

40. Strong passwords should be used following advice published at http://www.gsmlondon.ac.uk/password and complying with the College's password policies of the General Information Security Policy at https://intranet.gsmlondon.ac.uk. Passwords must be changed at least every 12 months to maintain security.
41. All IT equipment under the College's care should be maintained in a secure manner in line with the General Information Security Policy and Security Manual. IT support personnel have a particular responsibility in this regard.
42. All devices connected to the College's campus wired network should run a currently supported operating system. 'Currently supported' means within the product lifecycle, i.e. the operating system must have been released, not preview or beta, and still be receiving security patches from the software vendor. All devices should have up-to-date operating system and application software security patches applied and where feasible anti-virus/anti-malware software installed, regardless of whether they are owned by the College or personally owned. For College-owned systems, these should be installed and configured according to Information Services' recommendations with auto updating enabled and following guidelines and policies defined in the General Information Security Policy.
43. Only those authorised to do so should install data or software onto College-owned devices and they should ensure it has been checked for viruses or other malware. Where necessary, administrative rights may be granted to permit users to install software on College devices following processes described at http://www.gsmlondon.ac.uk/is/itregs/ictpolicies/PC+and+Laptop+Admin+Rights. Users should not transmit files/data to others, without first checking for viruses or other malware.
44. Information Services reserves the right to disconnect any computer from the network that is discovered to be infected with malware (e.g. viruses, trojans), that is suspected of being compromised or being involved in activities in breach of these Conditions of Computer Use, or which does not have adequate virus-checking software installed. The associated password should be reset on an uninfected machine. Once cleaned, the device can be reconnected to the network.

Connecting equipment to the network

45. All devices connected to the College's network must be used in line with the College's approved policies and processes detailed at http://www.gsmlondon.ac.uk/is/itregs/equipreg.
46. No equipment connected to the network (whether College or user owned) should be used to extend or provide additional connections, for example via wireless transmitters or routers, unless approved for this purpose by Information Services.
47. User-owned computers have been authorised or registered using self-registration processes detailed at http://www.gsmlondon.ac.uk/is/itregs/equipreg must also comply with the additional Self-registered Equipment Terms and Conditions detailed at http://www.gsmlondon.ac.uk/is/itregs/selfregtc.
48. The College reserves the right to prohibit the use of equipment that is likely to cause interference on frequency ranges used by the College's wireless network.
49. The registered owner of a device will be held responsible for any inappropriate activity arising from that device. In the case of personally owned systems, the owner is responsible for ensuring that the device has up-to-date operating system and application software security patches applied, and – where feasible, meaning where such software is available – that up-to-date anti-virus/anti-malware software is installed.

Electronic mail

50. Only systems approved and provided by Information Services should be used by staff for email communications concerning College matters. For a list of approved systems see https://intranet.gsmlondon.ac.uk/
51. Staff must regularly access their College email account mailbox to manage any received correspondence.
52. Where practical, staff should not use College email systems for sending personal messages unrelated to College matters.
53. Email systems provide a written record and care should be taken when composing and sending messages to ensure that the intended meaning is conveyed and the message is delivered to the intended recipients. Good-practice guidelines on using email are published at https://intranet.gsmlondon.ac.uk/
54. Emails that infringe another person's copyright should not be passed on.
55. Anything sent electronically, including email, is susceptible to interception. Users should whenever possible avoid sending highly confidential or sensitive information by email. If it is essential to do so, the information should be

contained within a password-protected file attached to the message. The password should conform to the College's password policies and guidelines detailed at http://www.gsmlondon.ac.uk/password and should be communicated to the intended recipient by other means.

56. Users should never send their College password in an email. Any email that asks for your password is a hoax.

57. Before sending an email, users should assess whether the message is representing College views and whether the information is confidential, and make this clear within the message. A liability disclaimer and confidentiality statement should be added to the message if appropriate; links to recommended text for these are provided at https://portal.gsmlondon.ac.uk/

Only a user's College assigned email address will be used to send email messages from the College to the user. Undergraduate and postgraduate (PGT and PGR) students wishing to read their emails from the College using an external service provider's email system are responsible for changing the settings on their College email account so that messages are automatically forwarded to the external service provider's system. Staff should also be aware of the above. Students are reminded that the College requires them to be in a position to respond to any notice or communication directed to them within 48 hours of it being made available to them, i.e. of it being posted on a notice board, on their College email account or in their pigeonhole.

NOTE: Staff wishing to send or receive personal email messages while at work should use a web-based external email service such as those provided by Google, Yahoo, or Microsoft.

58. Users should note that their use of the College email system is not private and that while continuing to maintain the privacy of personal mail, the College reserves the right to inspect and disclose the contents of emails under special circumstances as declared in 'Monitoring and Privacy'.

59. Files downloaded from the internet, including mobile code and files attached to email, must be treated with the utmost care to safeguard against both malicious code and inappropriate material. Such files, or any others not known to come from a trusted source, must be scanned for possible malicious code before being opened.

Internet publishing

60. The College adheres to principles of academic freedom of expression. However, those publishing information via the internet should note the following.

61. Users should be aware that posting information to any extended group including discussion forums, websites, social media sites, news feeds and blogs, or even to a list of recipients, is publication. Likewise, placing information onto a computing system in such a way as to make it accessible to the general public via the internet is publication.
62. No item should be published using the College's IT facilities that could be considered defamatory, discreditable or injurious to the College's reputation, that in any way contravenes current legislation, or that could result in any violation of the Janet Acceptable Use Policy. The College reserves the right to remove or request the removal of any such material and to remove access rights to prevent further publishing of such material.
63. Students are advised to consult the guidance on the use of social media published by the Dean of Students' Office as part of its bullying and harassment policy.
64. Any social media accounts and blogs affiliated to the College must take note of guidance published by the College Marketing Team at https://portal.gsmlondon.ac.uk/ and should be confirmed and registered with the Social Media Co-ordinator via tweet@gsmlondon.ac.uk as soon as they are created.
65. Before creating a new website affiliated with the College, you must consult the Digital Marketing Team at digitalmarketing@gsmlondon.ac.uk and follow its guidance and advice to be compliant with College policy. (Domain registrations will be considered and approved by the Digital Marketing Team and set up and administered by ISD via digitalmarketing@gsmlondon.ac.uk.)
66. The College may allow users to publish information over which it does not exercise any specific editorial control. However, unless you have been duly authorised to act officially on behalf of the College, it disclaims all responsibility for such publications and asserts that you will be held responsible for any infringements of law or applicable regulation, and for any consequent claims.
67. Where the College has not duly authorised you to act officially on its behalf, you must make clear that the views you express are your own and do not reflect those of the College or your individual School/Department. An explicit disclaimer should be included unless it is clear from the context that the author is representing the College or their School/Department. A standard disclaimer for addition to emails sent to external parties is available from https://intranet.gsmlondon.ac.uk/is/itregs/userguide/emaildisclaim.

68. You should ensure that any information you post on a College website is accurate and reviewed regularly (at least annually).

Use of services provided by others

69. If a service provided from outside the College is accessed by means of College facilities, users must also abide by that provider's conditions of use, code of conduct, policies or rules regarding the use of that service.

70. So that the College may comply with its licences for access to electronic resources (including databases and electronic journals), users must ensure the security and confidentiality of the electronic resources made available to them. In addition, users must ensure that any information derived from these resources is used only for the purpose defined in the licences, which includes non-commercial use only. Copies of these licences, which include full details of copyright restrictions, are available for inspection on application to the main Library.

71. The College is not liable for any financial or material loss to an individual user in accessing the internet for personal use. In particular, if you connect to external services using the College network and internet connection to carry out personal transactions such as purchase of goods or banking transactions, the College accepts no liability for those transactions, or for the security of any personal data transmitted.

Staff providing IT and service support

72. It is recognised that during their duties College staff providing IT support, or support for College-provided services, may have access to confidential information stored on computer systems. IT support staff also have special responsibilities as regards ensuring security of computer systems within their care. The conditions detailed below apply to all staff who provide IT support, or support for IT-based services and are in addition to those conditions listed elsewhere in this document.

73. Support staff will only actively seek information on a computer that is relevant to the work being carried out. Specifically they will not open files or emails on a user's computer, or in a user's computer account, unless necessary to solve the problem being investigated.

74. Support staff will maintain strictest confidence and will not divulge confidential information stored on a computer or in a computer account to others unless they suspect illegal activity or activity that contravenes the Conditions of Computer Use. Note: access to College centrally provided services such as email

and the network is monitored by IT support staff to maintain service efficiency and prevent problems. Such monitoring does not involve access to a user's computer account/resources unless authorised by the Assistant Director Strategy, Policy and Compliance or a member of the ISD Management Team, who will be responsible for overseeing such activity.

75. When a computer system is temporarily removed from a user's office to carry out work on it, IT support staff will ensure that the equipment is housed in a secure environment so as to prevent unauthorised access or theft.

76. Users' passwords will not be reset or divulged to others, except:

(a) where a reset is required for security reasons;

(b) where the user is unable to access their account because they have forgotten their password. In this case their password will be re-set and communicated to them;

(c) where a member of staff is absent and the Head of Department or Department, or their deputy, requests access to the user's account to carry out the business of that Department. In this case the password will be reset and conveyed to the appropriate person requiring access.

77. Support staff should not expect or ask a user to disclose their password.

78. 'Administrator' passwords should not be divulged to anyone except authorised staff engaged in support work where that work cannot be done without such access. Additionally, administrator privileges should not be assigned to any individual's IT account unless they are authorised to undertake work which requires this. An auditable log must be maintained of those issued with administrative passwords and the password reset whenever a person is taken off this list or leaves the College.

79. Permissions and privileges giving access to a user's computer, IT account, email account, or stored files and data must not be altered unless for good reason and with the user's knowledge and agreement, except where requested to do so for investigative purposes and with approval of the appropriate people.

80. IT support staff will not connect to a computer over the network without the prior agreement of the system owner or, in their absence and for operational reasons, the Head of the Department concerned or their deputy. This includes mapping network drives with administrator passwords and connection to PCs using remote desktop tools. If such a connection is required for investigative purposes, this must be authorised by the Assistant Director Strategy, Policy and Compliance or a member of the ISD Management Team.

81. IT support staff will only dispose of unwanted computers or data storage devices using the disposal service included within the College's Managed Service for PC Procurement contract. This service will guarantee that all data is deleted in such a way that it cannot be recovered.

82. If a computer or data storage device is transferred within College for use by another user or Department, any data stored on the system should be erased in line with HMG Infosec Standard 5 Enhanced criteria to ensure any previous owner's information cannot be recovered.

83. IT support staff are responsible for the good security of systems within their care and for encouraging where possible the good security practice of individuals using those systems. Policies and controls as detailed in the General Information Security Policy and in the Security Manual should be adhered to. If a user asks them to do work that they feel would compromise security, they should advise against this and if appropriate discuss it with their line manager or the user's line manager.

Visitors

84. The Conditions of Computer Use as they apply to visitors to the College may be summarised as follows:

(a) Visitors must not intentionally contravene these College Conditions of Computer Use in any way.

(b) If residing in College residences, visitors must not contravene the Self-Registered Equipment Terms and Conditions at http://www.gsmlondon.ac.uk/is/itregs/selfregtc

(c) A visitor's IT equipment must not be used on the College network without having been registered for this or authenticated via Eduroam.

(d) A visitor's computer must not be connected to the College network without up-to-date anti-virus/anti-malware software being installed and operational.

(e) Visitors must not try to run any software whose use is prohibited by the College, either on their own system connected to the College network, or on College-owned systems.

(f) Visitors must not disclose to anyone else passwords that have been allocated to them for the purpose of authorised access to College IT and computer systems.

(g) Visitors must not take any action to circumvent any College security control that is in place.

Monitoring and privacy

85. The College reserves the right to monitor use of the College network, associated telecommunication systems and the Internet by users and, if necessary, to withdraw access if it is felt this is being used excessively for purposes unconnected with or to the detriment of work/studies.

86. Routine monitoring takes place for maintenance, fault-finding purposes and enforcement of these Conditions of Computer Use, which may reveal unencrypted data and sites visited by users to operational staff. More detailed monitoring may also take place if there are reasonable grounds to believe a user has committed a criminal offence or has otherwise breached the Conditions of Computer Use.

87. Users should note that College IT facilities are provided primarily for College work, study and business purposes and that while continuing to maintain the privacy of personal information, the College reserves the right to process information stored on College IT systems, including the content of emails, web pages and files under the following circumstances:

    (a) To locate substantive information that is required for College, School or Department business.

    (b) To determine the dates when email, network and the campus card were last used in support of the missing person's protocol.

    (c) To set up an automatic reply or forward mail if members of staff are unexpectedly absent or have gone on leave without making forwarding arrangements.

    (d) In an investigation triggered by indications or allegations of misconduct, misuse, or illegal activity reported by managers or colleagues, monitoring processes, or some other legitimate and objective complaint or incident.

    (e) To respond to legal processes, or to fulfil the College's obligations to third parties or in other exceptional circumstances, e.g. medical emergency.

    (f) Electronic correspondence will only be intercepted in exceptional circumstances, and only with lawful authority.

88. All access and monitoring will occur in line with the Human Rights Act 1998, Data Protection Act 1998, Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and the Regulation of Investigatory Powers Act 2000.

Breaches of these Conditions of Computer Use

89. If there are reasonable grounds for suspecting that a user is engaging in activities that breach the Conditions of Computer Use, the College reserves the right to investigate fully, including directly monitoring the user's use of the network and computing facilities. The College also reserves the right to withdraw (temporarily or permanently) the authority of any user to use any system in such circumstances. Direct monitoring of individual use or withdrawal of services in such circumstances may be authorised only by the Director of Information Services, or their authorised deputies, in consultation with the Human Resources Division (or the Academic Registrar's Office in the case of student users).

90. A breach of these conditions of use may lead to disciplinary proceedings or disconnection from the data network. In serious cases, this could result in dismissal for staff or exclusion for students. (A significant breach of these conditions of use is likely to be regarded as serious or gross misconduct.) A breach of these conditions of use may also be a criminal offence. The College will report the matter to the police where appropriate.

91. The College reserves the right to charge users for the restitution costs, as decided by the College, regarding any damage they deliberately cause to any IT facilities.

92. The College also reserves the right to seek reimbursement of any costs arising from legal actions taken against the College caused by any failure of a user to comply with these Conditions of Computer Use, where this has been due to deliberate neglect, deliberate avoidance or criminal act.

Reporting computer misuse

93. Computer misuse is any activity involving the College's IT facilities that is illegal, contravenes these Conditions of Computer Use, or has any of the following characteristics:
    (a) Compromises the security of the College's IT systems or its data.
    (b) Breaches the College's Information Security Policies.
    (c) Results in a formal complaint from a member of the public or another member of the College.
    (d) Is part of a Police enquiry.

94. If a member of the College becomes aware of such activity, they have a responsibility to report this to either the Information Service's Assistant Director Strategy, Policy and Compliance, or in their absence the Director of Information Services. If appropriate, they will begin investigative action and will inform and

engage with the Human Resources Division, Academic Registrar's Office or Head of [add]

Advice and support

95. Information Services is responsible for ensuring regular monitoring and updating of these Conditions of Computer Use on behalf of the College.

96. If you need any advice and/ or clarification of these Conditions of Computer Use, please contact the IT Helpdesk in the first instance:

- Tel. 020 8516 7800 (ext. 1501) or e-mail itsupport@gsmlondon.ac.uk

Document review and communication

97. Information Services is responsible for the review and communication of these Conditions of Computer Use. There will be an annual mini-review to keep up to date with changes in legislation and technology, and a major review every five (5) (5) years. The review will be overseen by a team consisting of representatives from Information Services, the Human Resources Division and the Academic Registrar's Office. The IT and Computing Forum, IT support managers, student representatives and staff trade unions will also be consulted as necessary. Revisions to the Conditions of Computer Use will be submitted to the Information Strategy and Services Committee for their consideration and approval as a College policy before the start of each academic year.

98. The Conditions of Computer Use will be published on Information Services' website at http://www.gsmlondon.ac.uk/is. All registered IT account holders will receive an email at the start of the academic year reminding them of the Conditions of Computer Use and their obligations.

Policy legal framework

The management of information security and the use of computers at GSM London are framed by UK legislation including:

- Data Protection Act (1998)
- Counter-Terrorism and Security Act 2015
- Regulation of Investigative Powers Act (2000)
- Human Rights Act (1998) • Computer Misuse Act (1990)
- Prevent duty guidance (2015)