Heythrop College

The Specialist Philosophy and Theology College
of the University of London

Computing Regulations

(these regulations apply to all users of Heythrop IT resources)

Contents

1. Introduction

The information in this handbook applies to all users of Heythrop College IT services. It must be read in conjunction with the College's other polices.

In case of a difference in interpretation between Heythrop College computing regulations and any other regulations/policies (internal or external to the College) which may also apply, then the most restrictive meaning will be deemed to be the regulation in force. In all matters that may require subjective interpretation (e.g. indecent images), the College's judgement will be binding.

These regulations apply to use of Heythrop College IT facilities, including (but not limited to), computers and other IT equipment, the wired and wireless networking facilities, software, the college website and other internet based facilities.

The College is required by law to bring to the attention of all staff and students the following notices.

Regulation of Investigatory Powers Act 2000

Heythrop College draws to the attention of all users of the College's data and telephone networks the fact that their communications may be intercepted as permitted by legislation.

Legislation allows the College to intercept without consent for purposes such as recording evidence of transactions, ensuring regulatory compliance, detecting crime or unauthorised use, and ensuring the operation of their telecoms systems. The College does not need to gain consent before intercepting for these purposes although we need to inform staff and students that interceptions may take place.

Please note that this has always been the College practice; in the course of their normal duties some staff have the authority and indeed duty to carry out certain monitoring activities in order to ensure the correct operation of telecommunications systems. This does not imply that all communications are monitored, just that they **MAY** be for the above purposes.

Data Protection Act 1998

The College holds user registration data and other information on the use of the College's computer systems and network; this includes log-in and log-out times, printing logs, World Wide Web cache logs, attendance and network traffic logging.

While normally only used for resolving operational problems, these logs will be analysed down to the individual user where a breach of the Regulations or other misuses and abuses of the facilities is suspected. This information may be passed to a third party for further analysis or where legitimately requested.

The information will also be used to communicate with individuals to alert them to malfunctions within the College IT facilities or to request action to correct the malfunctions which may be putting the normal operation of the IT facilities in jeopardy.

In addition, statistical analysis may take place, which does not identify any individual, to provide management information on computer lab, attendance, software, printing, cache, network and general computer usage.

2. JANET Acceptable Use Policy

Any use of the College computing facilities via JANET (www.ja.net) is also subject to their Acceptable Use Policy (http://www.ja.net/company/policies/aup.html). An extract from version 10 (April 2008) is provided below.

> *Unacceptable Use*
>
> *11. JANET may not be used by a User Organisation or its Members for any of the activities described below. (**Note 3**)*
>
> *12. 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. (**Note 4**)*
>
> *13. Creation or transmission of material with the intent to cause annoyance, inconvenience or needless anxiety.*
>
> *14. Creation or transmission of material with the intent to defraud.*
>
> *15. Creation or transmission of defamatory material.*
>
> *16. Creation or transmission of material such that this infringes the copyright of another person.*
>
> *17. 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.*
>
> *18. Deliberate unauthorised access to networked facilities or services. (**Note 5**) (**Note 6**)*
>
> *19. Deliberate activities having, with reasonable likelihood, any of the following characteristics:*

- *wasting staff effort or networked resources, including time on end systems accessible 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 JANET(UK) 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" or other harmful software via JANET.*

Explanatory Notes

3. The list of unacceptable activities in this section is not necessarily exhaustive. In accordance with clause 9, the use of JANET for any activity which may reasonably be regarded as unlawful is not permitted. The purpose of this section is to bring as clearly as possible to the reader's attention those activities most commonly associated with the abuse of a network.

4. It may be permissible for such material to be received, created or transmitted where this is for properly supervised and lawful purposes. This may include, for example, approved teaching or research, or the reception or transmission of such material by authorised personnel in the course of an investigation into a suspected or alleged abuse of the institution's facilities. The discretion to approve such use, and the responsibility for any such approval, rests with the User Organisation.

5. Implicit authorisation may only be presumed where a host and port have been advertised as providing a service (for example by a DNS MX record) and will be considered to have been withdrawn if a complaint from the provider of the service or resource is received either by the User Organisation or by JANET(UK). For all other services and ports, access will be presumed to be unauthorised unless explicit authority can be demonstrated.

6. Where a User Organisation wishes to commission or itself perform a test for vulnerabilities in its IT systems (for example, via "penetration testing") this, as an action authorised by the User Organisation, will not be a breach of clause 18. However, the User Organisation should inform the JANET CSIRT, in advance of the test, of the source, nature and timing of the test. This is to avoid wasting the time and resources of the CSIRT in investigating the perceived attack on the User Organisation, or automatically blocking it

10. 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. Any breach of industry good practice (as represented by the standards of the London Internet Exchange), or of the Acceptable Use Policies of other networks, that is likely to damage the reputation of the JANET network may be regarded as a breach of this AUP.

3. Accessing other networks

Where Heythrop College IT facilities are being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of the College AUP. Any breach of industry good practice (as represented by the standards of the London Internet Exchange), or of the Acceptable Use Policies of other networks, that is likely to damage the reputation of the Heythrop College network may be regarded as a breach of this AUP.

4. Authorised Users & Usage

No person shall use the computing facilities of the College without due authorisation being given (usually by issue of a personal username and password). Passwords are **NOT** to be revealed to any other person.

No person shall by any wilful or deliberate act damage or otherwise jeopardise the integrity of the computing equipment, systems, software, or the work of other user.

No person shall run, obtain or distribute any software by illegal means using College computing facilities. For avoidance of doubt, users of College equipment may **only** run software that has been authorised in advance (a full list is available on the College web site). When attaching personal computer equipment to the College network users are prohibited from using software of services that does not have an appropriate licence.

Users must comply with the Computer Misuse Act 1990, three specific offences are defined:

> *Definition 1: Unauthorised Access to Computer Material, including using another person's identifier (username) and password, without proper authority, in order to use data or a program, to alter, delete, copy or move a program or data, or simply to output a program or data (for example, to a screen or printer); laying a trap to obtain a password; reading examination papers or examination results;*
>
> *Definition 2: Unauthorised Access to a Computer with intent, including gaining access to financial or administrative records;*
>
> *Definition 3: Unauthorised Modification of Computer Material, including destroying another user's files; modifying system files; creation of a virus; introduction of a local virus; introduction of a networked virus; changing examination results; and deliberately generating information to cause a complete system malfunction.*

Any person who wishes to use the College's computing facilities for private purposes (e.g. consultancy and other commercial activity which is unrelated to their study/work) must seek prior approval. This approval may be granted by the Dean of Undergraduate Studies (UG Students), the Dean of Postgraduate Studies (PG students), the Academic Registrar (Alumni & External Students) or the Principal (Staff & Governors).

Occasional personal use of the College computing facilities (including College email) is permitted so long as use is not excessive and does not disrupt or restrict usage by other legitimate users.

The staff of the College will at all times have authority to maintain good order in the use of the College's computing facilities and may suspend or exclude from their use any person who breaks these Regulations. They may report to the Principal (or other member of the Senior Management Team) a person responsible for serious or persistent misuse of computing facilities which breach these or any other Regulations. Such conduct by any student will be considered a breach of the College Terms and Conditions, such conduct by staff may be considered a breach of their employment contract. At all times staff reserve the right to report any suspected illegal behaviour to the appropriate authorities and may assist in the investigation of such behaviour.

The College reserves the right, at any time, without reason to suspend an individual's access to College IT facilities (this may include prevention of login, access to email and files).

5. Email & SMS (Text Messaging)

Email is a very important means of communication within the College. All members of the College must have and regularly use an email account as supplied by Heythrop College. Students are expected to check their email on a minimum of a weekly basis during term-time and ideally no more than fortnightly during vacations. Staff should endeavour to check their email regularly during term-time and occasionally during vacations/sabbaticals.

a) heythrop.ac.uk email

All staff will be given an email address in the form **<initial>.<surname>@heythrop.ac.uk** it is expected that this is the main email address they use when communicating on College business.

All students will be given an email in the form **<studentID>@heythrop.ac.uk** whilst registered with the College, this is also their computing username.

College email systems may not be used for any of the following:

- transmission of commercial material without specific approval,
- unsolicited messages to a large number of people (spamming),
- messages requesting recipient to re-forward thereby setting up a chain action (chain mail),
- messages likely to cause offence,
- messages purporting to come from someone other than the actual sender (spoofing),
- material advocating criminal activity or which may bring the College into disrepute,
- material which violates copyright restrictions,
- material which is defamatory or libellous,
- material which could be used to breach computer security or facilitate unauthorised access,

- material likely to prejudice the course of justice,
- personal data about a third party in contravention of the Data Protection Act.

All email is intrinsically insecure unless it is encrypted, therefore discretion should be used if information of a confidential or sensitive nature is being considered for transmission by email. A standard College disclaimer is added to all outgoing email

A user's email account and the data associated with it is private. Users must not intercept or read another user's email messages unless specifically authorised to do so. In the case of permission being given, for example, to a personal secretary to access email for a member of staff care must be taken to ensure that third party personal data is not compromised.

Systems administrators, or other computer staff involved in operational or networking aspects of the email service, must not monitor other users' email except in so far as this is a requirement of the normal course of their work. In all other circumstances such monitoring or reading of other users' email may only be carried out with the permission of the Principal or Vice-Principal. Requests for access to a user's account, for example in the case of long term absence of the user where information of importance to the business of the College is likely to be in the account, must be made in the same way.

The College reserves the right to access and disclose the contents of a user's email box only in accordance with its legal and audit obligations and for legitimate operational purposes. In such cases, if encryption has been used, the College will require that the encryption keys be made available in order to fulfil its right of access.

Email filtering

The College both as a service to its users and in order to protect its network applies various filtering processes to email before delivery to a user. The aim of the filtering is to remove viruses and to reduce the amount of junk email (spam) received by the user. However the College cannot guarantee 100% success in this filtering and it is possible that either some legitimate email is blocked or some unwanted email is not blocked. In general users should always be aware; that opening of attachments that are not expected may be harmful; replying to junk email (even to remove oneself from list) is not advisable; chain email should not be forwarded (in case of doubt please check with the College IT staff).

Text Messaging

The College uses SMS (text messaging) as an alternative method of communication with its students, and students must ensure that their mobile number is recorded correctly at all times with Registry. In general messages sent in this way will be more time-critical or important than communications by email.

The College may also communicate with its staff by SMS on an occasional basis.

6. Storage and Backup

The College stores and backups data (including files, emails and access logs) that passes through its network. This is done on a daily basis, however users should note that for non-critical systems this service is only offered as a 'best endeavours' service and users are responsible for ensuring that data they consider to be important is stored securely. Advice may be given on this on request by contacting the College IT staff.

For email messages sent from or received by the College mail hubs, a log is kept of the transaction (sender, receiver, date/time, subject etc.) but not the content. This data is kept for a minimum period of 1 month. Users are responsible for storage of their own email, both incoming and outgoing, within the limits of the file handling facilities available to them. The College, as part of its data storage policy, automatically backs up all user files on the central systems on a daily basis and retains back-up data for a minimum of 3 months.

7. Acceptable Use of Open Access Computer User Areas

The open access computer user areas are provided primarily to support students' academic work in the form of formal class work or private study. When not booked all such areas may be used, during the designated opening hours for that room, by any authorised user.

Open access computers can be in great demand, especially at busy times of the day during the teaching year. Using a computer for social or recreational purposes during these periods can deny it to someone who may have a more urgent, legitimate need.

All users are required to observe the following:

- During busy periods don't “surf” the Internet for recreational purposes (e.g. Facebook).
- During busy periods use email only for work-related activities: leave social emails for a less busy time.
- Minimise conversations in open access computer areas.
- When in an open access computer area, switch off all mobile phones (or turn to silent mode).
- Respect other users' requests for quiet.
- Help ensure the reliability of the computers by not eating or drinking at a computer.
- Respect the environment, don't leave litter, use the bins provided.

8. Printing

The College as part of its ethos believes that printing should not be chargeable. Thus when using college computing facilities users have free access to several printers. However it is the expectation of the College that this is to be used for the printing of documents relating to study or work. It is permissible to print short personal documents (e.g. email, shopping receipts, etc.), but this permission may be withdrawn at any time.

The College may use a system whereby users are given print credits, these are not chargeable, and are used for auditing purposes. A user may request additional credits from the help desk.

9. Wireless Networks

The College provides a number of wireless networks in order to facilitate internet and email usage by its users. The College provides these as an additional service to users and it cannot be guaranteed that these will be functioning at any point in time. All College computing regulations apply to this usage.

10. Intranets (Helios, HeVN, Hesperus)

The College operates a number of intranets. Access to these is granted only to specific users. All College computing regulations apply to this usage.

11. Electronic Coursework Submission (Students)

a) The College may make and may authorise third parties to make copies of any work submitted by you for assessment but only for the following purposes:

i. assessment of your work;

ii. comparison with databases of earlier answers or works or other previously available works to confirm there is no plagiarism; and

iii. addition to databases of works used to ensure that future works submitted at this institution and others are not plagiarised from your work.

iv. for teaching purposes within Heythrop College

b) The College will not make any more copies than are necessary for these purposes, will only use copies made for these purposes and will only retain such copies as remain necessary for those purposes. Where copies are made and retained for the purposes identified in clauses 11a-ii, 11a-iii and 11a-iv above, the College shall endeavour to ensure that no personal data is made available to any third party.

12. SENDA/DDA

The College makes its best endeavours to comply with provisions contained within legislation, in particular the Special Educational Needs and Disability Act (2001) and the Disability Discrimination Act (1995). These endeavours extend to the College IT services and users with specific requirements are encouraged to contact either the College Student Support Services or IT Services to ascertain if their requirements can be met.