

E-mail Policy for Staff

This Policy was approved by Council 23rd June 2005 and comes into force 1st September 2005.

0. Purpose

All use of e-mail within the College and from College e-mail addresses is subject to College Regulations. The purpose of this Policy is to supplement College Regulations by:

- making explicit the application of the College Regulations to e-mail
- highlighting legal issues relating to the use of e-mail
- defining College procedures in relation to staff e-mail accounts
- outlining the College's Policy on the monitoring of e-mail.

It is important to note that this Policy applies not only to College e-mail accounts but to any e-mail or other electronic messaging facilities (e.g. external e-mail accounts, newsgroups, web-based discussion forums, etc.) accessed via a computer connected to the College network.

This policy is concerned essentially with regulatory and procedural issues. Recommendations on good working practice are given in Computer Services Guide *Using the College E-mail System: Good Working Practice* (in preparation). There is a separate *E-mail Policy for Students*, which should be consulted by staff who need to understand the regulations and procedures governing student use of e-mail accounts.

1. Unacceptable Use

The term "unacceptable use" is used here, as with other institutions providing e-mail facilities, to refer to any use which could lead to disciplinary action.

1.1. *Unauthorised access*

E-mail facilities are provided to individual members of staff exclusively for their own use.

1.1.1. The following constitute unauthorised forms of access to College e-mail facilities and may be subject to disciplinary action:

- a) Permitting anyone else to send e-mail using the username or e-mail address you have been given**
- b) Sending e-mail using another user's username or e-mail address**
- c) Sending a message from a departmental or other non-personal e-mail account you have not been authorised to use**
- d) Accessing the personal mailbox of another user, except where mailbox sharing has been enabled by that user.**
- e) Attempting to disguise the e-mail address from which your message is sent or the identity of the sender.**

The first three of these also render the user liable to prosecution under the Computer Misuse Act 1990.

Note that infraction of 1.1.1a) may arise not only from deliberate action but also from negligence: leaving yourself logged in at a computer in a public area after you have finished using it, makes your username and e-mail account publicly available. For this reason, disciplinary action may be taken under College Regulation 24.3.3 against any user who compromises the security of the system by failing to log out after using a College computing facility.

Where access to the mail of another member of staff is required, this must be achieved by sharing mailboxes, *not* by sharing passwords (see 6.1.3).

1.2. Unauthorised purposes

Although staff e-mail accounts are primarily intended for use in connection with their work, reasonable personal use of these accounts is acceptable. Section 2 of this Policy provides guidelines on what constitutes reasonable personal use, but there are a number of activities which are not permitted under any circumstances in relation to College e-mail accounts or any College computer facilities.

1.2.1. The following are not permitted and could give rise to disciplinary action:

- a) Private use of the College's computer and e-mail facilities for commercial purposes unrelated to the business of the College or the wider academic community.**
- b) Sending unsolicited mail to multiple recipients, except where this relates to the business of the College or the wider academic community and is in conformity with the College's obligations under the Data Protection Act (1998).**
- c) Sending private mail from departmental or other non-personal e-mail accounts.**

Staff are not permitted to use the College's computer or e-mail facilities in relation to work for another employer, or to personal business activities. Exceptions to this may be allowed in individual cases, where special permission is given by the Director of Information Services.

For some staff, the distinction between College and private communication may not always be clear, but use is permitted only where commercial activities relate directly to the member of staff's role as an academic or one supporting academic work. Staff, are not permitted to use their College e-mail address for outside free-lance or consultancy work, even where it relates to their academic specialism.

Staff who need e-mail for their own business purposes will need to have their own computer, Internet connection, and a non-College email account. If you are unsure whether a particular use is permissible or not, you should contact the Director of Information Services.

1.3. Improper content

Staff are expected to ensure that their use of e-mail does not give rise to criminal or civil proceedings and should note that a number of classes of content are classed as “improper” for this reason.

1.3.1. It is a disciplinary offence to send from a College e-mail account or from a computer connected to the College network any e-mail or other electronic message which is:

- a) Defamatory
- b) Obscene
- c) Racist
- d) Sexist,
- e) Bullying, or
- f) Threatening.

1.3.2. It is a disciplinary offence to send from a College e-mail account or from a computer connected to the College network any e-mail or other electronic message which:

- a) constitutes racial or sexual harassment, or
- b) might cause unnecessary distress to the recipient.

An e-mail message is, for legal purposes, treated as a publication, and is therefore subject to all the normal legal restrictions on publication, including copyright protection. Forwarding a message without permission could be construed as a breach of copyright.

1.3.3. It is a disciplinary offence to include copyright material in an e-mail message without the permission of the copyright holder

Of course, permission need not be sought where a message contains information obviously intended for forwarding or for wider dissemination, or where the original message was posted to a publicly accessible forum.

Note that the College’s disciplinary procedures may be invoked in such cases regardless of criminal or civil proceedings.

1.4. Unsuitable purposes

E-mail is not necessarily suitable for every purpose. Misaddressing may result in apparent non-delivery of the message; proof of sending does not constitute proof of receipt, which may be necessary in some situations;¹ data protection legislation makes it inadvisable to include certain types of personal information in an e-mail message.

¹ The “read-receipt” feature, which prompts the recipient to confirm arrival of the message, may be useful, though a recipient may refuse to acknowledge such a request so it is not a guaranteed method of ascertaining delivery.

- 1.4.1. Staff may not on their own initiative require or encourage students to use e-mail for the submission of any work which constitutes a formal part of student assessment.**
- 1.4.2. Coursework which constitutes a formal part of student assessment may be submitted by e-mail only where**
 - a) this is specifically permitted or required by the course regulations, and**
 - b) the submission procedure adheres to the published protocol for the electronic submission of coursework approved by Academic Board. ²**
- 1.4.3. In the case of Visiting Students who have returned to a home institution, Registry and the Examinations Office have discretion to permit the electronic submission of coursework or the electronic notification of examination results on an individual basis, where**
 - a) The alternative might seriously disadvantage the student**
 - b) It would not breach other regulations, and**
 - c) Appropriate security measures are applied.**

Under the College's *E-mail Policy for Students*, students are informed that electronic submission, unless specifically permitted or required under the regulations for the particular course, is deprecated and done entirely at the student's own risk. The College accepts no responsibility towards students for the non-delivery or "late" delivery, for whatever reason, of coursework sent via e-mail, except under the provision of paragraph 1.4.2. Computer Services cannot respond to requests from students or departments to provide proof that a particular message with a coursework assignment was sent at a particular time.

E-mail is not an appropriate communication medium for certain types of material. In particular, unencrypted e-mail is unsuitable for anything of a confidential nature. The difficulty of providing proof of sending and receipt makes e-mail inappropriate for contractual and similar matters.

Sending a e-mail message which contains information about an individual should be done with caution: under the Data Protection Act, such an individual might have a right to insist on seeing messages containing her or his personal data.

1.4.4. The following are not suitable for sending by e-mail:

- a) Any correspondence between a student and the College in a disciplinary matter or other formal dispute**
- b) Any message relating to staffing issues which includes personal details (e.g. performance, discipline, salaries, etc.)**

² There is currently no College protocol for electronic submission of coursework.

- c) Any opinions or facts concerning a person which it would be inappropriate to share with that person
- d) Any material relating to the content of examination papers
- e) Any message which includes examination or assessment marks where the student(s) to whom the marks relate is or could be identified
- f) Any material where there might be a contractual or other legal need to prove the identity of the sender, or to demonstrate the receipt of the message
- g) Messages to recipients who are not known to read their e-mail regularly.³

1.4.5. The College's Management Framework on Data Protection places specific obligations on individual members of staff, including "Avoiding as far as possible writing down (in electronic or hard copy form) opinions or facts concerning a Data Subject which it would be inappropriate to share with that Data Subject."⁴

2. Personal Use of Staff E-mail Accounts

2.1.1. Reasonable use of a staff e-mail account for personal e-mail is permitted.

However, private personal messages are not exempt from the general provisions of this Policy:

2.1.2. Any private message sent from College systems must be lawful and comply with this Policy.

In particular, the provisions of Sections 1.1 and 1.3 of this Policy apply to *all* mail sent from College e-mail accounts or from computers connected to the College network, and the fact that such a message may be private does not provide any immunity against disciplinary action in case of infringement.

2.1.3. Staff must ensure that any mail sent in a purely private capacity does not imply that it is being sent on behalf of the College.

2.1.4. Any member of staff using a College e-mail address for personal e-mail must ensure that he or she:

- a) does not allow it to interfere with the performance of their duties
- b) does not allow it to take priority over their work responsibilities

³ The existence of an e-mail address does not guarantee that the owner of that address actively uses it, or checks it regularly.

⁴ A "Data Subject" is an individual person about whom personal data is held.

- c) does not thereby incur unwarranted expense on the part of the College
- d) does not allow it to have a negative impact on the College in any way.

3. Privacy & Monitoring

3.1. Privacy

The College undertakes to respect the confidential nature of private messages as is required by law.⁵ However:

- 3.1.1. It is a condition of use that any member of staff using College e-mail facilities for personal messages accepts that the College cannot provide an absolute guarantee of privacy or confidentiality in respect of such messages.
- 3.1.2. Normally, any electronic message with a signature which includes a member of staff's job title or department, or the name of the College, may be regarded *a priori* as pertinent to College business and may therefore be excluded from the privacy guarantees given in this Policy.
- 3.1.3. Notwithstanding paragraph 3.1.2, messages that are identifiable by their message header, signature or folder as relating to activities which, although they may arise from the member of staff's employment, are not part of the business of the College will be regarded as private.

The most obvious application of this is to Trade Union matters, but it would also apply, for example, to any social activities which involve members of staff but which are not carried out as part of their job. Trade Union officers may wish to ensure that messages relating to union activity are signalled as such by an appropriate subject line or using a distinct signature, and that received messages are stored in a suitably named folder.

- 3.1.4. Staff sending mail to a College e-mail address should be aware that the sharing of mailboxes and arrangements for the handling of mail to absent members of staff may result in a message being read by someone other than the addressee.

This is particularly the case with senior staff whose mail may be dealt with by a secretary or PA on a regular basis.

Sections 3.2 to 3.7, below detail the circumstances in which the general guarantee of privacy may be overridden or compromised.

⁵ Human Rights Act 1998 <www.hms0.gov.uk/acts/acts1998/19980042.htm>. Article 8 covers "the right to respect for his private and family life, his home and his correspondence".

3.2. Monitoring

The interception and/or reading of e-mail addressed to individuals is generally contrary to UK legislation⁶ and the College does not monitor e-mail accounts of staff or students as a matter of course.

However, the law explicitly gives employers who provide e-mail facilities for the purposes of their business the right to examine the e-mail accounts of individual staff under certain circumstances, which include:⁷

- The investigation of potential breaches of the institution's regulations and policies relating to the use of electronic mail
- The need to preserve the security of the institution's systems
- The prevention or detection of crime.

The College therefore offers the following assurances with respect to the monitoring of staff e-mail accounts:

3.2.1. Monitoring of College e-mail accounts will be undertaken only in circumstances permitted by law.

3.2.2. Monitoring is carried out by systems staff only on the basis of explicit written authorisation from the Director of Information Services and the College Secretary.

A member of staff's line manager would normally be notified of monitoring, but the College need not notify or seek authorisation from either senders or recipients of messages monitored. Under normal circumstances, a member of staff whose mail has been monitored will be informed subsequently that their mail has been subject to monitoring.

3.3. Dealing with Absence

Staff e-mail accounts are provided primarily in order to facilitate the conduct of the College's business, and measures are therefore necessary to deal with e-mail in cases of staff absence. Section 6 of this Policy explains the arrangements a member of staff is expected to make in cases of leave or other planned absence. But staff should be aware that the needs of the College during an unplanned absence may compromise the general respect for the confidentiality of private messages.

3.3.1. In cases of unplanned staff absence, the College reserves the right to examine a staff mailbox for messages relating to the business of the College which require attention.

Normally, agreement for this would be sought from the member of staff, but where circumstances do not permit this, mail may be read in the absence of such agreement.

3.3.2. When a department requires access to the mailbox of an absent member of staff, the head of department must make a formal

⁶ Regulation of Investigatory Powers Act 2000
www.hms.gov.uk/acts/acts2000/20000023.htm.

⁷ The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (Statutory Instrument 2000 No. 2699)
www.hms.gov.uk/si/si2000/20002699.htm.

request to the College Secretary, who will authorise the Director of Information Services to make appropriate arrangements.

Departments making such requests are expected to have the explicit permission from the owner of the e-mail account or to include in their request an explanation why permission has not been obtained.

3.3.3. No member of staff must request or attempt to discover the password of an absent colleague in order to secure access to their mailbox.

This is a breach of College Regulation 24.3.2 and may lead to disciplinary action.

3.3.4. Staff authorised to deal with another person's e-mail in their absence are required to respect the privacy of personal messages, and to treat as confidential any private material inadvertently seen.

Respect for the privacy of the absent member of staff in these circumstances is not always straightforward, since it may not be obvious from the sender's name and the subject line that a message is of a personal nature. However, mailboxes which include the words *personal* or *private* in their names should always be treated as out of bounds in these circumstances.

3.4. Accidental Disclosure

One of the circumstances in which the confidentiality of e-mail messages may be compromised is when Computer Services staff deal with technical problems relating to e-mail:

- 3.4.1. Staff using College e-mail facilities for personal messages accept that Computer Services staff, when dealing with technical problems relating to system security or to mail delivery, may inadvertently be exposed to the content of messages stored on College servers.**
- 3.4.2. Computer Services Staff are required to treat as confidential any material in staff mailboxes inadvertently seen while dealing with technical problems.**
- 3.4.3. Notwithstanding the undertaking of confidentiality given in 3.4.2, Computer Services staff will report to the Director of Information Services any material inadvertently seen in these circumstances which appears to constitute a breach of this Policy.**
- 3.4.4. Staff who, because of misaddressing, receive mail not intended for them must report the misdelivery to the sender and respect the confidentiality of the message.**

3.5. Refusal of Delivery

- 3.5.1. In order to protect the College's computer systems, systems staff may put in place appropriate automated measures to prevent the**

delivery of e-mail messages which appear to represent a security threat.

Such measures will be general in their application and are not targeted to individual users or accounts. In such cases the non-delivery (and the reason for it) will be reported to the sender.

3.6. *Non-personal Accounts*

3.6.1. The privacy provisions of this Policy apply only to personal accounts attached to an individual staff username; staff using departmental and other general e-mail accounts have no expectation of privacy for messages.

Departmental and other general e-mail addresses are not intended for the personal use of individuals, and the contents of any mailboxes for such accounts may be examined by appropriate staff on the authority of the relevant Head of Department or other manager without reference to the individuals normally responsible for their day-to-day management.

3.7. *Compliance with Legislation*

3.7.1. In responding to requests for information under the Data Protection and Freedom of Information Acts, the College may be obliged to disclose the content of e-mail correspondence held on College mail servers, irrespective of whether the sender or the recipient has deleted the message from local inboxes. In such circumstances the rights of senders and recipients of e-mails to privacy have to be balanced against other legal requirements which may apply in the context of particular messages.

3.8. *Privacy of E-mail Addresses*

Anyone with a College username can look up the usernames of others, and within the College, therefore, the e-mail address of a member of staff or student is not confidential.

3.8.1. E-mail addresses of staff are not confidential, and requests from outside the College for the e-mail address of a member of staff may normally be complied with without formality or the explicit permission of the member of staff concerned.

However, in many cases it may be more appropriate to give a general or departmental address than the personal address of an individual.

Staff who, for any reason, need to have a confidential e-mail address should contact the Director of Information Services.

3.8.2. E-mail addresses of students are treated by the College as confidential, and requests from outside the College for the e-mail address of a student should normally be refused.

The appropriate response to an outside request for a student e-mail address is to:

- a) forward the request to the student, or
- b) instruct the enquirer to send their request by e-mail to *postmaster@gold.ac.uk*.

3.9. Assuring Privacy

3.9.1. Staff who wish to guarantee the confidentiality of a personal e-mail message should use an external e-mail account.

If this is done from a computer connected to the College network, all other provisions of this Policy apply, but the College will have no direct access to copies of messages.

4. Communicating with Students

While many students have e-mail accounts with outside mail systems, the lack of guaranteed levels of service on such accounts and the fact that they may be blocked or terminated without notice makes them unsuitable for use in relation to a student's studies. Also, mail sent from a student's College e-mail address provides assurance that the sender is in fact a student of the College and to some degree authenticates the identity of the sender. The *E-mail Policy for Students* therefore specifically bans the use of such accounts for College purposes in the following terms:

"Students are expected to use their College e-mail account for all e-mail relating to their studies, and not to use other e-mail accounts for this purpose." (1.6.1)

Since a College e-mail account can be accessed from anywhere on the Internet, students not on campus should not have any difficulty sending messages from their College e-mail address, and this requirement should not restrict the ability of students to use e-mail in connection with their studies.

The *E-mail Policy for Students* has the following implications for staff:

- 4.1.1. Staff should send all e-mail for students to their College e-mail addresses and not send e-mail to external e-mail accounts for this purpose.**
- 4.1.2. Staff responding to mail from a non-College e-mail address claiming to be from a current student**
 - a) **must be satisfied as to the identity of the sender**
 - b) **may refuse to respond to the substance of a message until resent from a College e-mail address.**

Identifying the sender may be unproblematic for academic departments, since staff will generally be receiving mail from individual students known to them. However, support departments should insist on the use of a College e-mail address as proof of identity.⁸

- 4.1.3. Staff should not use their own non-College e-mail accounts to send e-mail to students.**

⁸ Of necessity, the Computer Help Desk, however, will respond to messages reporting problems with College e-mail accounts sent from any e-mail address.

Staff are reminded that not all types of content are suitable for sending by e-mail – see Section 2 of this Policy.

5. Security

As mentioned in Section 1.4 of this Policy, “Unsuitable Purposes”, staff are discouraged from sending sensitive or confidential material by e-mail. E-mail is not in fact less secure than the post – it is simply that it is not obvious when a message has been read by someone other than the intended recipient.

There are two main ways in which a message could be seen by someone it is not intended for:

- Someone could gain unauthorised access to the mailboxes of sender and/or recipient
- It could be wrongly addressed.

The first of these is addressed by the provisions of Section 1.1 of this Policy and by College Regulations relating to computer use. However, breaches of confidentiality are more commonly caused by lack of care in the addressing of messages:

5.1.1. Staff must take reasonable steps to ensure that they have the correct address for the intended recipient.

The foolproof method for doing so is to use the Reply function with an incoming message. Within College, the e-mail address of any registered user can be found by using the *finger* command on the UNIX system (see "Finding E-mail Addresses" in the Information Services Handbook). Staff e-mail addresses, and instructions on how to use them, are given in the College Staff Directory (on-line at <www.gold.ac.uk/staff-directory/>). Staff who are uncertain about acceptable formats for e-mail addresses should consult Computer Services Guide *Correct Formats for E-mail Addresses* (in preparation).

The only way to guarantee that an e-mail message is not read by unauthorised persons is to encrypt it. While there are encryption systems which offer very high levels of security, these cannot currently be provided on the College mail system. However, any file created in a word-processor can be password protected and sent as an attachment; archiving utilities such as Winzip or Stuffit can also be used to create password protected files. As long as you do not include the password in the message, this will be at least as secure as the post.

Paragraph 3.4.4 covers the receipt of mis-addressed messages.

6. Leave and Other Absence

Since staff e-mail accounts are provided primarily for the conduct of the College's business, staff are expected to make provision for the expeditious handling of incoming mail during any planned absence longer than a few days.

6.1.1. Staff must ensure that there is appropriate access to their e-mail account for material relating to their College responsibilities during leave or sickness.

There are five ways to do this:

- a) monitor incoming mail and forward messages to a colleague, where appropriate.
- b) monitor incoming mail and place relevant messages in a shared mailbox
- c) have incoming mail automatically forwarded to another College e-mail address
- d) share the INBOX and other relevant mailboxes with an appropriate colleague or colleagues.
- e) Set up an autoresponder to inform the sender that the recipient is not able to deal with the message promptly and to provide an alternative contact address for urgent matters.

Options a) and b) might be appropriate and practicable in case of study leave, but are unlikely to be feasible, or particularly welcome, in cases of serious illness. They may also not be feasible where study leave involves remote field work. Forwarding (documented in Computer Services Guide C4.13 *Redirecting E-mail*, on-line at <www.gold.ac.uk/infos/cs/guides/c413.pdf>) has the disadvantage that mail is removed from the mailbox of the original recipient, who will therefore be unaware of the message.

In such cases, sharing mailboxes is the preferred solution:

6.1.2. Staff who are not intending to monitor their incoming mail during planned absence must set up the sharing of their INBOX and other appropriate mailboxes.

Paragraph 3.3.2 of this Policy states the procedure to be followed where it is not possible for the member of staff to set up mailbox sharing in person.

6.1.3. Under no circumstances must a member of staff reveal their password to a colleague to facilitate dealing with e-mail during an absence.

This is a breach of College Regulation 24.3.2 and may lead to disciplinary action. Computer Services will not give departments the passwords of absent staff members so that incoming e-mail can be dealt with.

6.2. Autoresponders

Autoresponders, while convenient for the member of staff on leave, give rise to a number of problems, and they should therefore be used carefully.

6.2.1. Staff who set up or make use of automated response facilities (an "autoresponder") to indicate to e-mail correspondents that they are away from College and unable to respond to e-mail until a given date, must ensure that any such automated response gives specific contact details, preferably a College e-mail address, for any matters that cannot wait until their return.

6.2.2. Staff who are subscribed to mailing lists must ensure that mail from such lists is suspended during the operation of an autoresponder.

6.2.3. Computer Services reserve the right to disable without prior notice any autoresponder which gives rise to an unacceptable

load on the mail server or to significant complaints from recipients.

- 6.2.4. Autoresponders may be set up only for individual staff e-mail addresses. It is not permitted to set up an autoresponder for a departmental or other general e-mail address.**

7. Retention

- 7.1.1. Staff must retain copies of any messages which may need to be referred to in future.**

In principle, any incoming or outgoing e-mail which relates to the business of the College should be archived for future reference. However, much e-mail, particularly within the College, is not of lasting importance and can safely be deleted.

Messages which need to be retained but are not relevant to current day-to-day matters should be archived by copying them to disk and deleting them from the mail system. It is suggested that, for most areas of College activity, messages more than two years old do not normally need to be immediately accessible on the mail server. Leaving large numbers of non-current messages on the mail server has an unnecessary detrimental impact on the College's e-mail resources.

However, Data Protection legislation requires that data relating to individuals should not be retained for longer than is necessary, which means that retaining *all* mail indefinitely may lead to breaches of the Act.

- 7.1.2. Staff must not retain longer than is necessary copies of messages which include information about identifiable individuals.**

Detailed advice about what should be archived and how long it should be retained are beyond the scope of this Policy. Staff should seek advice relevant to their areas of responsibility from their line-manager. In general staff should retain any e-mail message which might need to be referred to again and which, if sent by post, they would have filed.⁹

- 7.1.3. Staff who use private e-mail accounts in relation to College business are required to ensure copies of messages are archived in such a way that they can be retrieved by the College if necessary.**

8. Leavers

- 8.1.1. Staff e-mail accounts are immediately frozen on the termination of employment with the College.**

This means that it is not possible for leavers to receive incoming mail, send mail, or access mail stored in mailboxes.

⁹ This paragraph will need to be replaced by a reference to a documented archiving policy when one is available.

8.1.2. All incoming messages for staff who have left will be bounced, i.e. returned to the sender as undeliverable.

Leavers will need to inform personal correspondents of a change of e-mail address. The College Web site provides departmental and other non-personal e-mail addresses so that senders of bounced messages can find an appropriate contact within the College.

8.1.3. Any messages remaining in the mailboxes of staff who have left the College's employ are the property of the College. The College is free to examine these, make them available to other members of staff, and delete them as necessary.

Leavers are strongly advised, before the end of their employment, to archive and/or delete from their College mailboxes all messages in account which they regard as personal. By leaving messages in a College mailbox after the termination of employment, a member of staff assents to the College's having unrestricted access to them. However, under Section 7 of this Policy, "Retention", staff must not delete messages which the College may in future need to refer to.

8.1.4. Where circumstances prevent a member of staff deleting personal messages before the termination of employment, or where the freezing of a leaver's e-mail account would cause significant problems for a department, either the leaver or the Head of Department should request the Director of Information Services to make suitable transitional arrangements.

9. Infringements & Complaints

9.1.1. Any use of e-mail which appears to be unacceptable in the terms of this Policy or which in any other way appears to contravene College Regulations may give rise to disciplinary action.

Misuse should be reported immediately to the Computer Services via the e-mail address: abuse@gold.ac.uk. Messages sent to this address are seen by the System Manager, who is responsible for the security of e-mail in the College, and who will report any misuse to the Director of Information Services for action. Alternatively, misuse can be reported in person to the Computer Services Help Desk, who will refer the matter to the Director of Information Services.

Any member of staff who receives e-mail from outside the College which might be regarded as offensive or potentially illegal, should report the matter to Computer Services. This is best done by forwarding the message to abuse@gold.ac.uk. (Forwarding an offensive message to this address does not constitute an offence.) The Computer Services will take up the issue with the management of the site from which the mail was sent.

Note that this applies only to College e-mail accounts – the College cannot take action where offending e-mail is sent to a non-College e-mail account even where this is accessed from a computer in College. In such cases, the provider of the e-mail account is the appropriate recourse.

Where a complaint is received which relates to a message sent by a member of staff, the Director of Information Services will institute investigation and refer the matter for disciplinary action, if warranted, under the relevant College procedures.

10. Useful E-mail Addresses

| | |
|-------------------------------|--|
| <i>helpdesk@gold.ac.uk</i> | For general enquiries about the use of e-mail in College. |
| <i>abuse@gold.ac.uk</i> | For reporting any misuse of e-mail. |
| <i>sysadmin@gold.ac.uk</i> | For enquiries about any security-related matters. |
| <i>secretariat@gold.ac.uk</i> | For enquiries about the use of email specifically in relation to Freedom of Information and Data Protection legislation. |

Queries about this Policy and its implementation should be addressed in the first instance to the Director of Information Services.