



E-MAIL USAGE STATEMENT

Introduction

1. This statement supports the [Communications and Information Systems Use Policy](#), setting standards on appropriate e-mail use.
2. City of London e-mail access is provided in order to facilitate efficient working.
3. E-mail is considered an insecure method of communication. Before transmitting any City of London data via e-mail due regard must be given to the sensitivity of the data and the impact of it being intercepted, mis-delivered or it being later forwarded by a third party. Published IS advice should be followed e.g. [IS Advice on Data Security](#), [IS Advice – Risk Analysis for Sensitive Data](#).
4. E-mails are potentially disclosable to third parties, including the subject of a particular e-mail, under the [data protection and/or freedom of information legislation](#).
5. This statement applies to all those who use the City of London Information Systems (IS) core infrastructure to access the City of London e-mail system.

General Principles

6. The City of London allows limited personal e-mail usage e.g. during breaks or before / after shift. This includes the sharing of non-work related e-mails between work colleagues.
7. E-mail must not be used to send or receive statements, images, information or sounds which:
 - bring the City of London Corporation into disrepute;
 - are potentially offensive, abusive or defamatory especially in accordance with our [equal opportunities](#) and [employee complaints](#) policies;
 - solicit or carry out business activities for personal gain;
 - display or disseminate pornography;
 - view or participate in any illegal activity;
 - divulge material to unauthorised third parties;
 - non-work related subscriber information e.g. mailing lists;
 - contain information of a sensitive or contractual nature.

This is not an exhaustive list.
8. Inappropriate or excessive e-mail use may lead to action being taken either through the [disciplinary policy](#) or as a criminal offence (see also [Communications and Information Systems Use Policy](#)).
9. Consideration must be given to limiting email distribution lists to those recipients



who need the information. E-mails should never be sent to 'everyone' in the organisation.

10. Recipient lists of e-mail messages should be carefully checked to ensure they are correct prior to sending to protect sensitive or protectively marked information.
11. Consideration must be given to the general housekeeping of Inboxes, in line with the [Records Management](#) principles.
12. Consideration should be given to using 'short-cuts' to documents on shared drives instead of attaching files.
13. Employees should minimise the possibility of introducing malicious software to the City of London's IS (e.g. unsolicited or non work related attachments should not be opened).
14. Access to some attached file types may be restricted based upon operational needs or to ensure system security.
15. All e-mails must be responded to in line with the [Service Response Standards](#).
16. Consideration must be given to the management of your inbox e.g. use the 'out of office assistant', particularly where [Freedom of Information](#) requests are likely to be received.
17. E-mail access may be withdrawn if it is abused.
18. If information as set out in [paragraph 7](#) is received, it must be reported via line management immediately.
19. Appropriate training is available via [Desktop Training Services](#).
20. Advice on this statement can be obtained from departmental HR.

Responsibilities

21. Line managers will ensure that e-mail usage does not negatively impact upon operations within the City of London.

Monitoring

22. E-mail usage will be monitored corporately, with issues being provided to departmental Chief Officers to manage, in line with the [employee data protection policy](#) and the [code of conduct](#) (see also [Communications and Information Systems Use Policy](#)).