E-mail for Users

The following notes provide some hints and tips about the use of e-mail. They cover the content and format of e-mails, sending and receiving attachments, courtesy and general housekeeping tips.

Common Courtesy

Always consider the feelings of recipients when composing e-mails. Good manners are also important when dealing with incoming e-mail.

E-mail should be read at least once a day if possible. If users are away for long periods, try to let people know.

Think whether an acknowledgement of receipt would be appropriate (and be aware that automatic acknowledgements are not always reliable).

Say 'Please' and 'Thank you'.

If an annoying e-mail is received, do not react with a 'knee-jerk' response that is likely to make the situation worse. It is possible that the sender did not realise the effect their message would have. Alternative actions could be pursued. These include:

- go and talk to the sender
- wait until the next day before replying
- delete the e-mail and ignore it.

Requests for action should be acknowledged and it may be appropriate to also confirm completion of the task. Reply to questions as soon as possible, even if it is only to confirm that help cannot be provided.

Do not forward chain letters - they clog up the network.

Content

There are many ways of composing e-mails and some are better than others. It is worth remembering that it is easy to offend recipients, particularly when a message has been composed in a hurry. Many users of e-mail have discovered the hard way that messages meant for the eyes of one individual have been broadcast to a wider audience because the 'reply to all button' was used in error.

It is good practice to:

- use a descriptive title in the subject field - but do not rely on people having read the title. If it is important, repeat the subject in the text (cut and paste is quick and easy)

- keep the message short and to the point but remember that the reader may need some background information. You may need to explain the following, which are also useful if mail goes to the wrong person, as the context lets them guess who it was really for and pass it on:
- why the e-mail is necessary
- why you are sending it
- why they are receiving it.

Do not use:

- abbreviations unless you are sure your reader will understand them
- all capitals - it makes the message harder to read and equates to 'shouting' in the e-mail world
- all lower case - it looks sloppy.

Format

Ideally an e-mail should not exceed a screen of information and should be simple text only, as formatted mail will probably not appear the same on all machines:

- keep the line length to about 60 characters
- use plain text - no special characters (even pound signs can cause problems)
- do not use formatting: no colours, bold, italic, underline, etc.
- do not use special fonts: rely on the one provided by your mail software
- do not use tabs: if you want a table effect, use a fixed-width (non-proportional) font that uses the same space for all characters including blank spaces, such as Courier or Mishawaka, and insert spaces.

In most cases it is best to send a minimally-formatted message with line ends manually inserted, as the damage done to such messages when received in a richer environment is less than the effect of a complex message that cannot be displayed properly.

Signature File

Most packages allow users to set up signature files. These files should be short (not more than four lines) and professional.

Sending Attachments

Do not attach something that can easily be sent in the text of the e-mail (meeting agendas etc.):

- only send attachments if it is clear that the intended recipient can read them (make sure their word processor/spreadsheet software can read the file)
- if the attachment is large, it is well worth doing a trial with a small one first
- mailing lists generally object to attachments - consider whether the item can be published somewhere else and let readers choose when (and whether) to fetch it
- in general, do not attach html files - give the web address
- give attachments meaningful names (and the correct extensions).

Unlike the text of an e-mail, all attachments are sent encoded. Although with PC mailers this happens automatically, there are several coding formats in use. If the mailer at the sending site is incompatible with the mailer at the recipient's site, it will not be possible to read any attachments. Attachments can also contain viruses and some people will therefore not accept them.

It is generally acceptable to send attachments within an organisation, but remember that people who do not use the same e-mail program may have problems. When sending attachments to other people, a MIME (Multipurpose Internet Mail Extensions) compliant encoding format is most likely to be readable. In Internet mail the MIME standards RFC 2045 Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies, and others specify how to assemble a message.

Text may be encoded if it contains special characters or features. The parts of a message (e.g. some typed text and an attachment) are linked together into a single object that will pass through all Internet mail systems without damage, and reversing the MIME processes allows the recipient's mail program to recover the various parts, but different mail products will present the delivered message with different appearances and behaviours. MIME ensures that all the parts of a message are delivered, but not that they will be displayed identically on the receiving machine. Try to configure the sending program to avoid:

- proprietary or obsolete encodings such as 'binhex' or 'uuencode'
- sending '8-bit' characters without encoding ('quoted-printable' (QP) and 'base64' encodings cover most needs)
- sending both plain and encoded versions
- encoding simple text ('US-ASCII') for which no encoding is necessary.

The process of encoding a document or file for attachment, and of assembling the message that includes it, is quite complicated and can easily result in large messages even when sending very little information.

Before sending any document or file, check that it does not contain a virus. The mail program used may be able to do this automatically, provided anti-virus software is kept up to date.

Privacy

E-mail is not a private or secure medium. Remember that messages may be read by people other than those intended to receive them, by accident or malice; and that a received message may not be what it seems either in its origin or its contents. The sort of messages received from regular correspondents will be familiar, and this is a good guide to their authenticity.

If it is important to send a message that remains private then it will have to be encrypted, subject to regulations at the sending and receiving organisations. Readily available products include PGP® (Pretty Good Privacy®), GNU Privacy Guard and S/MIME (Secure/Multipurpose Internet Mail Extensions). The same technology and products ensure that the contents of a message have not been changed and to some extent confirm the identity of the sender. There are, of course, other media for communication such as post, fax and telephone that can be used instead or can provide verification of a received e-mail

message.

When sending a message to multiple recipients, consider what personal or other information is being revealed. If the addresses are entered in the usual and simplest way, each recipient will see the addresses and possibly the names of all the others, and they may not have agreed to that. Most mail programs have a Blind Copy facility (Bcc:) that allows the inclusion of an address to which the message will be delivered but which will not appear in any delivered copies. This facility does not work in exactly the same way in all mail systems and programs, and local support staff should be asked for detailed advice (or test with a few friends who have agreed in advance). Note too that the Bcc: recipients will not normally see their addresses in the copy they get, and they may not understand why they have got the message.

Forged E-mails

Any part of an e-mail message, including the From: address, can be forged, for example to commit fraud or distribute viruses. Any message that is unexpected or has unusual content should be treated with suspicion, even if it appears to come from a known source. In particular beware of opening attachments to such messages, as these may contain viruses, backdoors or other hostile code. If there is any doubt about the authenticity of a message, consult your local support staff. It may be appropriate to delete suspect messages unread, even though this runs the risk of losing a legitimate communication. When writing messages yourself, include some obviously 'human' text: do not just send blank messages with an attachment as these may well be deleted unread by recipients who are concerned about viruses.

When replying to an e-mail, remember that it may not have been written by the person from whom it claims to come.

Receiving Attachments

Attachments in almost any format can contain viruses. All machines belonging to JANET-connected organisations should therefore be running a virus checker and any suspect items received should be checked before they are opened. If there is any doubt whether an attachment is genuine, do not open it without seeking advice from your local computer support staff.

Replying

When replying to an e-mail, ensure that text taken from the original message is clearly distinguished from the text forming your reply. Most mail clients can automatically insert a > character before each line of the original.

There is currently no general agreement over whether replies should come above, below or interleaved with the original message. There is no right answer here and in general users should comply with the norm of the group with which they are exchanging e-mails. It is however advisable to type the points in the reply close to the points in the original message for clarity. The guiding principle is to consider the convenience of the intended reader(s) rather than that of the sender. One widely recognised style is to show each point (or part of it) from the original separately, followed by your comments in response to that point. Blank lines

are usually enough to separate points.

When replying to e-mails:

- check the subject field is still relevant
- include ticket numbers in correspondence with help desks including the JANET Service Desk and JANET CSIRT;
- check that the recipients are those for the message is intended - beware when using 'reply to all'
- delete unnecessary quoted text but leave in enough so that the reply makes sense even to a recipient who has not got the original - remember when sending a message to a help desk (e.g. the Janet Service Desk or Janet CSIRT) that the person who reads the reply may not be the person who sent the original message.

Housekeeping

Users can easily become overwhelmed by the volume of e-mail received. To keep it down to sensible proportions:

- make sure that the mailboxes for incoming and sent mail are cleared out regularly
- file what needs to be kept using a folder or similar filing system provided by the e-mail system and delete the rest, checking that they are not hiding in a 'Trash' or Deleted Items' folder
- consider unsubscribing from high volume e-mail lists if away for an extended period.

E-mail for Organisations

Existing and new JANET customer organisations may choose to operate their own e-mail systems and services, or to procure all or parts of them externally in various ways. In all cases there are some requirements that will ensure seamless interworking with other JANET-connected organisations and with the wider Internet community.

These notes are primarily intended for managers of e-mail services within JANET-connected organisations where either e-mail is being set up for the first time or major changes in the design or implementation of e-mail services are being considered. They may also be of interest to suppliers and others who provide or support e-mail services for a JANET-connected organisation.

Conventions

The RFC document 2119 Key Words for Use in RFCs to Indicate Requirement Levels provides a convention for the use of keywords such as 'MUST' and 'SHOULD' to indicate what degree of discretion is allowed (if any) in interpreting directions and requirements in this area.

Where keywords are presented in BOLD UPPER CASE, the conventional meanings of RFC 2119 apply in assessing whether e-mail services conform to those required for an organisation connected to JANET. Certain technical or management requirements may seem rather severe in using this interpretation, but MUST and similar keywords are only used where there is some specific and compelling need.

External View

E-mail Addresses

Required E-mail Addresses

Domain Nameserver

Message Format

Relaying

Gateways

Dial-up Accounts

Web-based E-mail

E-mail Addresses

Internet e-mail addresses are of the form:

`<local-part>@<domain>`

The domain name broadly distinguishes an organisation's network from all others in the Internet and possibly specifies some department or division within the organisation, and the local-part identifies a particular individual or role within the organisation. There are normally no spaces in either part, nor on either side of the '@' separator.

Most organisations connected to Janet are entitled to a domain in ac.uk (the imaginary domain college.ac.uk is used for illustration here). JANET(UK) publishes rules on the choice of domain names immediately below ac.uk which are explained in Section 3 of this manual.

Published destination addresses SHOULD be of forms such as:

`Fred.Bloggs@college.ac.uk`

simple and explicit, but may be hard to keep unambiguous

`f.bloggs@dept.college.ac.uk`

less personal identity revealed, more organisational structure

`fr03200@college.ac.uk`
no personal name included.

Addresses SHOULD NOT be of forms such as:

fredb-chemsrv2@ntserver2.chem.college.ac.uk [1]

in which local private information about usernames, machine names and possibly the operating system in use are visible. There are two kinds of difficulty with such addresses:

- they are not stable since administrative or technical changes can make these addresses misleading
- the information they appear to contain is of more value to someone considering breaching an organisation's security than to any legitimate user.

E-mail addresses SHOULD NOT be case sensitive. If F.Bloggs is the local part of the published form of one of an organisation's e-mail addresses then it is normal to recognise forms such as f.bloggs, F.BLOGGS and even odd mixtures of case, and to regard them all as referring to the same address. Some people prefer to publish addresses that use capitals in the conventional way; some prefer all lower case. Whatever is published on paper will sometimes be entered incorrectly, and if the error is only to forget an initial capital then it is reasonable to expect the e-mail to be correctly delivered. Most e-mail software will default to this case-insensitive behaviour.

Addresses used in SMTP (Simple Mail Transfer Protocol) enable e-mail systems to route messages and to report failures. Addresses in the message header preceding the contents of the message are for the use of mail programs at the recipient's site, and enable them to do such things as show users who a message (ostensibly) came from and devise reply addresses.

Any address in the protocol envelope or the header of a message sent from an organisation's e-mail service MUST have a fully-qualified domain name (all components included up to top level .uk or similar), and MUST be valid for delivery.

MAIL FROM: (envelope) SHOULD be as published (but see the exceptions below)

From: header line MUST be as published

Sender: header line SHOULD NOT normally be used (but see below)

Reply-To: header line SHOULD NOT normally be used (but see below).

Exceptions: the requirements may be different for messages sent by an automatic process such as a web form or a mailing list.

Required E-mail Addresses

Organisations MUST implement the postmaster and abuse addresses for all domains within their management. RFC 2142, Mailbox Names for Common Services, Roles and Functions, describes other role addresses that should be provided under certain circumstances. If a site supports the facilities that any of those addresses provide, it MUST use the names prescribed for them.

Each organisation MUST arrange for a timely response to messages from JANET(UK) or its contractors sent to the postmaster and abuse addresses.

An organisation may, of course, wish to use alternative names as well. In these circumstances, e-mail systems must support such aliases and the originator that is specified in e-mail sent from role accounts must be valid and appropriate. Equally important, e-mail to these role addresses must be routed to one or more individuals who have the skills and resources to deal with it.

It is quite acceptable for the same individual or team of individuals to be responsible for messages addressed to more than one role.

Domain Nameserver

The IP address of a sending mailer SHOULD have a PTR (PointTeR - address to name) record in the IN-ADDR.ARPA. zone of the Domain Nameserver. The JANET Technical Administration Group can advise who has the delegated authority to make entries for a site network if this is not clear.

The sending mailer HELO (EHLO in Extended Simple Mail Transfer Protocol (ESMTP)) SHOULD be fully qualified and SHOULD correspond to an A (Address) record in the Domain Nameserver that matches the mailer's IP address.

Domains and subdomains for which the domain name of the appropriate inbound mailer differs from the domain name in e-mail addresses MUST have MX (Mail eXchanger) records in the Domain Nameserver indicating the mailer.

Message Format

The header part of every message sent from a JANET-connected organisation MUST meet the requirements of RFC 2822 Internet Message Format.

This states that the following lines are mandatory:

Date:

From:

To:

(see E-mail Addresses above).

The header SHOULD also include a Message-ID: line. The headers of messages sent from an organisation may or may not have Received: lines, depending on the software used and

the structure of the e-mail service. It may be possible to use Received: lines to identify the person originating each message (see Audit Trail below).

Timestamps in Date: and Received: header lines MUST be accurate to one second or better, with the correct time zone indicated. Timestamps SHOULD use the format +0100.

The Date: line is usually supplied by the user program that generates the mail messages, and it may be necessary to maintain the accuracy of clocks on numerous desktop or public computers. Various network technologies have proprietary ways to synchronise clocks within a network. The JANET Network Time Service enables an organisation to keep its network's time in step with those of other organisations on JANET and throughout the Internet.

Message-ID: and Received: are not usually shown to recipients, so deficiencies in these header lines may not easily be spotted.

Messages MUST conform to the MIME specifications in RFC 2045 Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies and related RFCs (possibly by having no MIME features at all).

Relaying

It is notionally possible for an e-mail message to travel by a single Internet connection from the computer on the sender's desk to the recipient's computer, with no other computer or service directly involved. In practice this is very rare and most users of e-mail are familiar with the idea that their messages travel in distinct hops, first within the sending organisation that has one or more mail servers, perhaps between service providers outside the sending or receiving organisation and then through servers close to the recipient.

A function of most Internet mail servers is to accept messages from some places and pass them to other places. In cases where the server makes no important change to a message, this is called relaying and all major e-mail server products provide such a facility. It is essential to configure this relaying in a secure way, allowing some combinations of source and destination but denying others.

In most cases only a very small number of systems will be expected to send e-mail out from the organisation, and very few will be expected to listen for incoming mail connections (SMTP, TCP port 25). The sending and listening systems need not be the same but they will all be known to and managed by staff responsible for the organisation's e-mail as a whole. Systems with this external access in either direction are exposed to open relaying attempts, and such attempts will only be defeated by a combination of technical and administrative arrangements.

The organisation's router or firewall SHOULD reject outbound packets to port 25 (the port used to send e-mail) at external addresses and inbound packets to port 25 at internal addresses, except for the above sending and listening managed mailers.

All e-mail systems with port 25 (SMTP) accessible from outside the organisation MUST be configured so that they will reject attempts to relay incoming messages through the organisation's mailers and back to the outside, except where such messages are explicitly authorised (see Dial-up Accounts below).

Similar considerations apply to TCP port 587, which RFC 2476 RSVP Operation over IP

Tunnels assigns for message submission.

For further information, see Section 6 of this manual.

Gateways

Some e-mail systems use open Internet standards such as SMTP, POP3 (Post Office Protocol3), or IMAP (Internet Message Access Protocol) throughout and will have no basic difficulty meeting the criteria listed here.

Other systems are primarily designed for use within an organisation. They can offer features not available in the Internet at large by a variety of proprietary techniques. However, in order to exchange e-mail with other organisations they need a gateway system that behaves exactly like that of a native Internet e-mail system as described above. The gateway system accepts messages from the proprietary e-mail system that are intended for outside Internet addresses and vice versa, and in each case makes any changes necessary to the messages concerned.

In such an environment the external behaviour of an organisation's e-mail (including message formatting and control of relaying) is almost entirely determined by the gateway. While this should in principle make management easy, many gateway products have poor implementations on their Internet side and each detail mentioned needs checking carefully.

Dial-up Accounts

An organisation may wish to allow its e-mail users limited access when they are away from their normal place of work. They may be at home, connected through a dial-up ISP, away at a conference, working with colleagues at another organisation or on holiday using an Internet café.

Organisations that use a proprietary e-mail system may find it impossible to offer this type of access. If the e-mail system uses open standards then there are a number of security issues, including the danger of operating an open e-mail relay as mentioned above. However, the main difficulty is authentication of individual users.

There is nothing in the most common open e-mail standards (POP3, SMTP) that will allow a site mailer to differentiate securely between a genuine user working from home, and a spammer or other abuser able to forge addresses. Both will attempt to connect to the site mailer from another network. An authorised user will be acting legitimately in preparing e-mail that looks as if it comes from an organisation domain, whereas identical address details from the spammer will be a forgery.

The normal advice to users is to send e-mail through their ISP's outbound mailer instead. The ISP normally has additional knowledge, such as the telephone number from which the dial-up call originated, and can in most cases justify the relaying required even if the user chooses to use their organisation address from home. If dial-up access is important for an organisation and its users, any claims by a supplier that a standard on-site product will get it right without leaving an open e-mail relay in the site network or the supplier's should be checked very carefully.

Web-based e-mail (see below) overcomes most of the problems. Other approaches using the

SSH (Secure Shell) and SSL (Secure Sockets Layer) protocols or proprietary secure connections, possibly in conjunction with an IMAP message store, are technically satisfactory but it is difficult to ensure that the end-user client software on which they depend is available in arbitrary external places.

Web-based E-mail

The approach of Hotmail® and many other service providers, particularly where there is no payment for the e-mail service, is to make a web browser the interface to all user e-mail facilities - authentication, reading, composition, sending and storing in folders. The e-mail system then comprises:

- a web server supplying a variety of forms for the tasks that a user can perform (web forms are pages with provision for user input)
- an authentication database against which one of the forms will validate users
- a message store that certain of the forms will manipulate to support an 'Inbox' from which each user can read their own incoming e-mail, and usually folders named by each user to allow them to organise their mail as they wish
- an external mailer that delivers incoming and internal e-mail to message stores, and formats and transmits outgoing messages.

For resilience and ease of management in all except the smallest services, the functions may be spread across two or more computers. Benefits include:

- the complete absence of e-mail software and data (messages) from all end-user computers
- concentration of management and technical resources for e-mail at a central system or collection of systems
- access to organisational e-mail (both reading and sending) from other locations.

Against this:

- the software is relatively complex and needs significant management
- it may be difficult to integrate existing user databases
- fewer features and facilities may be available to end-users than through dedicated e-mail software
- the service may interact more slowly with users than dedicated e-mail software
- some service providers are particularly vulnerable to malicious activity, Hotmail® for example having been broken into on several occasions.

An organisation considering obtaining a web-based e-mail service from an external supplier should ensure that it can meet all requirements for the appearance of outgoing mail, for the management of user accounts, and for usage reports. A free public service is unlikely to do so.

Internal View

E-mail Addresses

Audit Trail

Distribution Lists

Privacy

User Support

Service Scaling

Service Agreement

E-mail Addresses

All addresses used in outgoing messages MUST be valid and MUST have fully-qualified domain names. User e-mail programs SHOULD provide some address book or similar facility so that users need only supply short or easily remembered versions of addresses, or can select from a list. This is not the same as allowing mail programs to supply a default domain, which is less satisfactory and should not be used.

It is highly desirable that all the addresses used internally are the same as those published for external use, so that users do not need to choose which address to give to their correspondents. Organisations using proprietary systems for internal e-mail may find it difficult or impossible to arrange this.

Even where internal e-mail uses open Internet technology, there may be operational or historical reasons for the use of addresses that are different from the standard ones published. For instance, an organisation may have departmental or location e-mail servers and it may appear more efficient in network and machine resources to route e-mail directly between them by using addresses that include the names of those servers. The danger then arises that one of these internal addresses will escape to the outside world; organisations using this system should check that this is acceptable. The outgoing e-mail system or systems may be able to rewrite internal addresses to a suitable external form; or sites may have to accept that such addresses will start to be used for incoming mail. In this case special arrangements of MX records are likely to be needed to ensure that messages are delivered.

Audit Trail

Each organisation MUST adopt software and management procedures that make it possible to identify the person responsible for sending each message, independently of any information in the message itself that an end-user might supply falsely. This might be achieved in various ways:

- record an IP address in the message header along with the timestamp (possibly as a Received: line) and refer to access logs
- record an authenticated login in the message (only a partial solution)
- ensure that e-mail system logs are adequate and are not lost or damaged.

It is recognised that such technological procedures alone offer no assurance that the person using an account name and password at any particular time is or was authorised to do so. Organisations MUST therefore also publish clear instructions to all e-mail users about security of accounts, passwords, use of shared or unattended computers and other related matters.

Software and management procedures that result in a log of all messages sent out from the organisation MUST be adopted. The log must be retained for a suitable and agreed period (e.g. three months). The logs MUST be kept secure against unauthorised examination, alteration or accidental loss.

Janet or their contractors MUST be able to contact organisation e-mail administrators if any difficulty arises. The Janet Service Desk maintains a list of technical contacts, with telephone numbers. Depending on the nature of the enquiry, Janet may use the postmaster role address or the person identified in the RIPE database, and it is desirable that all these contact details are kept up to date.

Distribution Lists

An e-mail system SHOULD support the expansion and management of internal distribution lists. This allows individuals within an organisation to correspond easily with all staff or students, or all individuals in particular departments. Internal lists SHOULD NOT otherwise be accessible to mail sent from outside the organisation.

Most e-mail products will support lists, possibly by purchasing and installing additional software or components.

Check that:

- there are satisfactory arrangements for managing membership of internal lists
- access to internal lists is controlled.

Normally only members of the list will be able to send messages to it, but for some lists it may be desirable to extend this to certain managers or others inside an organisation, or even to certain individuals or roles outside the organisation.

Privacy

The organisation MUST publish internally a privacy statement setting out the circumstances in which e-mail and access logs and stored messages will be made available to persons or agencies other than the originator and recipients of the messages concerned.

The requirements of the Data Protection Act and the Regulation of Investigatory Powers Act will influence the content of this statement.

User Support

Users can expect support of various sorts:

- routine requests for changes to their account details
- information on the status of the e-mail service

- advice on the e-mail software they use
- advice on reports (often failure reports) from the e-mail system or from somewhere else
- action on what they perceive as abuse through the e-mail service, including both UBE and abuse that appears to be personal
- advice on good practice in using e-mail
- advice on the use of e-mail to access external services (e.g. mailing lists)
- advice on the interaction between the organisation's e-mail service and dial-up or other connection services they may wish to use
- information on an organisation's policies and procedures with regard to relevant current legislation, such as data protection, retention and destruction of data, or handling of requests from law enforcement agencies
- directions on security and acceptable use with appropriate reference to the JANET Acceptable Use Policy.

Much of the advice and information will be best provided through internal web pages or other documentation. Maintaining a list of FAQs (Frequently Asked Questions) is likely to be effective.

Where the user support function is separate from the operation of the e-mail service, communication between the two activities must be adequate. This is likely to be particularly important if an organisation is spread across two or more physical locations, or if all or part of the e-mail service is outsourced.

Service Scaling

The system or systems providing an e-mail service for a small organisation can be very simple, whether provided in-house or outsourced. Elements should include:

- a firewall barring access to unused ports on e-mail systems
- a central computer accepting incoming e-mail connections
- a central computer sending e-mail outside the organisation
- a central computer storing delivered e-mail for users to read
- computers and software with which users read and compose their e-mail.

For more information see the JANET Technical Guide Designing Reliable Mail Systems.

The central functions can be combined in a single system. Indeed, one computer may be able to manage parts of the e-mail system for several organisations, and this arrangement is quite normal for an outsourced mail service.

For a great variety of reasons, very few Janet-connected organisations have e-mail systems as simple as this. The need for gateways (for resilience in case of certain failures, for operation across multiple locations, for management within separate departments) and the size of an organisation all increase the complexity of the service. It is not practicable to give general advice on scaling for these conditions. The Janet Service Desk can provide assistance to organisations that require specific comment on a proposal. FE organisations and specialist colleges may also consult their JISC RSC for advice.

Service Agreement

Whether an e-mail service is resourced internally or from outside, both providers and users of the service need to be clear about what to expect.

Where the service is provided by an outside contractor, an organisation will normally have the most critical items closely linked to the agreement under which the contractor does the work. Headings might include:

- capacity of the service
- performance of the service (time taken for messages to pass through the system and network)
- availability of the service (and of certain specific parts of it)
- assurance of security
- response to requests for changes
- response to fault reports
- escalation and penalties.

For internal support, this may be regarded as documentation of the service or may be included in Quality or other documentation.

Where facilities are provided away from the site or networks, each of the headings may have an impact on internal e-mail as well as external traffic. This may affect the way in which some of the risks are assessed.

Links
[1] mailto:fredb-chemsrv2@ntserver2.chem.college.ac.uk