



Information security guideline

Email security

Sending emails

1. You are personally accountable for the content of all emails that you send. The spell checker may spot typing mistakes but it will not remove sentences that you will later regret having said! Choose your words carefully and remember that emails can easily be saved, printed and forwarded. They are increasingly being used as evidence in court so be especially careful to avoid libel/defamation or unnecessary disclosure of sensitive information.
2. The corporate email systems check that email addresses are valid but cannot check that you have addressed an email to the correct person. Take extra care when addressing sensitive or important emails and avoid responding to mailing list addresses if you only meant to reply to a single individual on the list. It's best to follow the process shown below:



3. Ordinary emails are more like postcards than letters. They can be read by IT people responsible for the email and network systems, just like the postman can read your postcards. Policies and procedures provide a degree of privacy for internal emails but emails sent over the Internet should be considered more or less public. Encryption is the *only* way to guarantee privacy of sensitive emails and *must* be used when sending confidential information including personally identifiable information and trade secrets. **Call the IT Help/Service Desk or contact the Information Security Manager for advice on email encryption.**
4. Email, especially Internet email, is not completely reliable. Emails sometimes go astray, get delayed or blocked by spam filters. It is also possible for someone to receive an email but deny having received it, and even "read receipts" do not absolutely guarantee delivery. Do not rely on email alone to authorize important business processes or transactions, such as contracts. **DO NOT AGREE TO CONTRACTUAL ISSUES BY ANY MEANS WITHOUT EXPLICIT AUTHORITY TO DO SO FROM MANAGEMENT.**
5. ALL emails sent via the Internet must have the approved disclaimer appended (this is done automatically by the corporate email system).

Receiving emails

6. The contents of unencrypted emails may be altered in transit. The "From:" address is only a guide to who *might* have sent an email and is easily altered by spammers and forgers. Emails encrypted using digital certificates are much harder to forge but it's always possible that someone other than the authorized person was at the keyboard. Don't rely on the sender.
7. Avoid opening attachments or clicking links in emails from unknown senders. They may be infected with viruses or Trojans. Report spam and offensive content to IT Help/Service Desk.

Further information

Call the IT Help/Service Desk immediately to report email security incidents. Visit Information Security's intranet website for more information on email security including encryption.