



Company Email Policy Draft

<<Company>> EMAIL USAGE POLICY Draft

1.0

Information must not be transmitted internally or externally which is beyond the bounds of generally accepted standards. This includes, for example, material which could be considered offensive or discriminatory; pornographic or obscene, defamatory or libellous or any other material which is otherwise abusive or contains illegal content prohibited by law or regulation or which brings <<Company>> into disrepute or which contravenes <<Company>> policies. Information is understood to include text, images, sound and video; transmission is understood to include printing information and sending information via email. Electronic harassment of any kind will not be tolerated by the <<Company>> and will be subject to the terms of the Etiquette at Work Policy. In particular, with respect to defamatory or libellous statements about another internal or external party, it should be noted that emails are discoverable documents in legal actions and may be used in evidence.

1.1

All material contained on the email system belongs to the <<Company>> and staff should not consider messages produced/received by them on <<Company>> equipment/software (owned or licensed) to be secure. The confidentiality of email cannot be assured and, in addition to the right of <<Company>> to monitor contents, staff should be aware of the possibilities of intended or accidental onward transmission to others beyond the original addressee(s). Furthermore, it is possible to retrieve deleted emails from back-up files intended to assure system integrity and reliability.

1.2

Security regarding access to the email system is of paramount importance as indicated in the Regulations. User identities and personal passwords must not be shared with others and staff should be wary of providing their email addresses to external parties, especially mailing lists.

1.3

Staff transferring or receiving files or attachments from external sources should note that <<Company>> system automatically checks downloaded material for viruses. However, in the event that a virus is suspected, the file or attachment must not be opened and the matter must be reported to the IT Department immediately for inspection and action.

1.4

<<Company>> email users are required to use this communication tool in a responsible fashion and to observe the related Regulations. <<Company>> provides the email system for the purposes of conducting <<Company>> business and it may not be used for personal gain/business activities unrelated to <<Company>> operations. Staff must not use the system to promote an external cause or fundraising campaign without advance line management permission.

1.5

Reasonable personal use of the email system is permitted, subject to the approval of Heads of Department and the constraints and conditions set out in this Policy and the Regulations. Heads of Department may define the level of use, as appropriate, in their areas. Personal use must not interfere with the operation of <<Company>> services, involve cost implications for <<Company>> or take precedence over the user's job accountabilities.

1.6

Authorisation to use the <<Company>> PCs at home or <<Company>> software on home PCs will be withdrawn on the termination of the employee's contract of employment and computer records of emails sent and received will be destroyed after a suitable period of time by the IT Department

1.7

<<Company>> has limited file storage capacity and has quota restrictions in place for certain individuals / departments which are heavy email users. It is essential that the following guidelines about email storage are adhered to otherwise it is possible that the email for everyone within <<Company>> will be affected.

What must all staff do?

1. Empty your deleted items folder regularly.
2. Do not store duplicate copies of documents such as PDF documents or image documents. Important documents should be stored locally on your hard disk or in your shared network folder, should they need to be backed up off site.
3. Personal documents should be stored on your local hard disk and should be backed up to floppy disk or USB drive if they are important.
4. Ensure that emails are archived at a fixed time period, each year for example and stored locally on your machine or on the server email archive.
5. Housekeeping of your emails is very important and should be done on a weekly basis.
6. Ensure that the IT department is aware of any additional storage requirements.