Topics > Business Procedures > Information Management and Technology Systems: Model Policies

# Internet Use: Staff Policy

## Policy Statement

This email and internet use policy has been developed to provide guidelines for staff relating to the acceptable use of the organisation’s email and related services and facilities.

The policy applies to all full-time and part-time employees of the organisation as well as agency and locum staff.

This organisation understands that inappropriate use of the internet or of email can lead to viruses entering computer systems, potentially damaging systems and compromising data security. The policy of the organisation is to control such risk by putting anti-virus technology in place and by establishing rules of safe and responsible internet and email usage that all staff should adhere to.

## Background

This organisation operates an internal and external email facility and provides access to the internet through its office and mobile computers or hand-held devices for those staff who require it.

## Use of Email and Internet by Staff

1. Email for staff is only available to registered users of the organisation’s computer network.
2. Email will be made available to all staff who require it as part of their work. Requests for an email address and for access to a computer should be made to the network administrator.
3. Staff must not send confidential/service user-identifiable information through unsecured email systems — when using email the principles of the Data Protection Act 2018 should be adhered to at all times.
4. Staff must be aware that many email systems are not 100% secure and confidentiality can be compromised, especially when using web-based email systems.
5. Staff must be aware that email carries the same legal status as other written documents and should be used with the same care.
6. Staff must be aware that email facilities employ complex technology which is not 100% reliable and therefore they should not rely wholly and solely on them for critical business processes.
7. It is strictly forbidden to send email messages that contain offensive, libellous, pornographic or harassing statements or language, particularly in respect of race, national origin, sex, sexual orientation, age, disability, religious or political beliefs. This includes jokes that may appear humorous to some, but offensive to others. Remarks sent by email that are capable of amounting to harassment may lead to complaints of discrimination or harassment under the Equality Act.
8. It is strictly forbidden to use the organisation’s computers or email system for the transmission of unsolicited commercial or advertising material, chain letters or other junkmail (often referred to as “spam”) of any kind, to other people or organisations, other than where that material is embedded within, or is otherwise part of, a service to which the organisation has chosen to subscribe (ie a facility for reporting junk or suspect email).
9. It is strictly forbidden to use the organisation’s computers to access websites that contain offensive, libellous, pornographic or inappropriate images or materials or to contribute to the development of such sites.
10. Staff should always report incoming “spam” or unsolicited email by using the appropriate facilities in their email system to identify and isolate it. Suspect email attachments should never be opened or passed on.

## Computer Viruses

Viruses can damage computer systems, destroy data, cause disruption and incur considerable expense for the organisation.

1. Staff must not independently load software onto their computers and all software installations must be arranged with the network administrator.
2. All computers and hand-held devices used in the organisation should have virus protection installed that scans email and files automatically. It is an offence for any member of staff to interfere with the running of these programmes. Where a privately-owned desktop computer or laptop is being used the owner must have the machine checked by the network administrator and make every effort to ensure that up-to-date anti-virus software is being used.
3. In order to prevent the spread or establishment of computer viruses, staff should never open an email attachment connected to an email from a source that they do not recognise and trust.
4. Staff must never transmit by email any file attachments which they know to be infected with a virus.

## Personal Use of Email and Internet

Although personal use of email facilities and the internet is discouraged, limited personal use will be permitted provided that the content of the message is appropriate, ie is not likely to cause offence, and websites visited are appropriate. Employees should regard this facility as a privilege that should normally be exercised in their own time without detriment to their job and not abused. Inappropriate or excessive use may result in disciplinary action and or removal of facilities.

Staff should be aware that both private and business use of email and the internet will be subject to monitoring.

Staff should not use the organisation’s email facilities to pursue commercial or business interests of any sort.

## Action in the Event of a Breach of the Standards of Acceptable Use

In circumstances where there is assessed to be a breach of the standards of acceptable use, as described above, the organisation will, as a first action, act promptly to prevent continuance or repetition of the breach, for example, by withdrawing email or internet access.

Indications of non-compliance with the provisions of the email policy will be investigated, as appropriate, in accordance with the organisation’s disciplinary procedures, as applicable to staff.

Subject to the findings of any such investigation, non-compliance with the provisions of the email policy will lead to appropriate disciplinary action, which could include dismissal on the grounds of gross misconduct. Furthermore, publication or sending some materials may not only amount to a disciplinary offence, but also a criminal offence, in which case the issue will be reported to the police for them to take appropriate action.

|  |  |
| --- | --- |
| Signed: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Date: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Policy review date: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |