Email and Internet workplace policies

SAMPLES

The internet and email opens your business up to a whole new world of communication and information. But it also opens your business up to potential problems. Your computer network can be open to viruses and corruption and your staff can abuse the technology available to them.

Email and internet policies are an important part of managing your employees. Your staff need to know what is acceptable practice in your orgainsation. As the acceptable level of access to internet and email differs from organisation to organisation, there is no one-fits-all policy. This is why this resource contains various sample policies that should be chosen and adapted to suit your organisation's needs.

The consequences of breaching the policy must be included in the policy. Employees need to know what is at stake if they breach the policy. The Employment Court will not take the employer's side in a dispute over dismissing an employee for a breach of policy if the employee did not know that he/she could be dismissed for the breach.

Your internet and email policy must be communicated to all staff. It is advisable to get a written acknowledgement from staff that they have read and understood the policy.

When developing your policy, you should consider the following:

- What level of access is reasonable for you to enforce on your staff. If you have a policy stating 'NO' personal emails or personal internet use, then this should be enforced. Consider if this will be realistic to enforce in your situation – perhaps it is worth considering a policy of limited personal use, out of work time only? Or be prepared to discipline any staff member for breaching the policy. If you let your staff get away with the 'odd' personal email, then this may become expected practice, and your policy may soon become not worth the paper it is written on.

- How is your email and internet traffic paid for? If you pay for the amount of traffic sent and received, it is a good idea to discourage the sending and receiving of large documents and graphics, particularly if they are not work related. These large documents and graphics can quickly add up to an expensive internet bill.

- It is worth considering having a standard disclaimer on the bottom of all emails (see Sample Policy 4). Recipients can change the content of the original email and/or forward it indiscriminately to others. Any liability can be minimised (but not eliminated) by the correct use of a disclaimer.

Sample policies for both email and internet use in the workplace are attached. These are provided as a guide only, and may need to be altered to suit your particular situation.

EMAIL POLICIES — SAMPLES

Sample Policy 1

- Email is a written means of communication. Please do not transmit anything in an email message that you would not be comfortable writing in a letter or memorandum. A rule of thumb is to assume that anything you may write could become public.

- *(Company Name)'s* network may be used for personal emails provided that such use does not interfere with work requirements.

- When sending emails using *(Company Name)'s* network, staff must ensure that laws related to privacy, defamation etc are not breached.

- Deleting an email message does not guarantee that it has been erased from the system. We retain back-up copies of all documents, including email correspondence, produced on the computer system.

- *(Company Name)'s* reserves the right to monitor email messages and disclose them to others. Please remember that email messages may be discoverable by opposing parties during litigation. Any inappropriate use of the email system could result in warnings or the termination of employment.

- Under no circumstances is pornography to be distributed via email.

- Breach of this policy: *(Company name)* may take disciplinary action, including dismissal, for any breach of this policy.

Sample Policy 2

Email is regarded as a key communication tool by *(company name)*. It has huge potential to speed up communication within the company, and to allow us to tailor the distribution of information to those who need the information concerned.

We also acknowledge the potential of external email to help us communicate better with our customers, suppliers, and stakeholders. The following protocols have been developed to help us manage our email effectively:

- Keep internal email brief – email is designed to speed up communication. Use abbreviations where possible.
- Use the address lists already supplied on the network (eg 'Everyone' for all staff), or create your own.
- Keep personal email to a minimum (email from every terminal is monitored, and excessive external use will be on-charged to the employee).
- Remember that graphics take a long time to transmit (and are therefore costly).
- Keep external or formal internal email as professional as you would a written memo.
- Offensive email, or email likely to affect the company's reputation, will not be tolerated (remember, usage is monitored through our network).

- Do not send highly confidential material by email unless procedures are in place to cope with the level of security required by that material.

Inappropriate use of the company's email system can amount to serious misconduct and may justify dismissal.

Sample Policy 3

Email is an essential business tool for *(company name)*, for both internal and external communications. However, use by employees of the email system can expose the company to liability, place extra burdens on the computer system, and breach the security of the system.

For these reasons, employees must:

- Avoid using the email system for personal use or to carry on any business activity not connected with their employment with the company. Electronic bulletin boards are provided by the system for employees' use for non-business purposes.
- Avoid sending messages with graphics attachments, as these slow the email system down and make it harder for our customers, suppliers, and stakeholders to communicate with us using the system.
- Keep external or formal internal email as professional as you would a written memo.
- Do not distribute any offensive or insulting email, or email likely to affect the company's reputation.

Email from every terminal is monitored. Abuse of the company's email system can amount to serious misconduct and may justify dismissal. Such abuse includes:

- Distributing offensive/insulting material or material likely to affect the company's reputation using the email system;
- Sending high volumes of personal email;
- Downloading from email personal software or files which may corrupt or affect the security of the computer system;
- Using other employees' terminals and/or log-ins to send emails (particularly if they are offensive); and
- Any other breach of this email policy that is serious or recurring after appropriate warnings have been given.

Employees must bring to senior management's attention any email received from external sources which is offensive or likely to corrupt or compromise the security of the company's computer system.

The IT team may filter employees' in-coming and out-going emails for content, and may block emails containing graphics files, very large documents, or offensive materials. Employees will be notified by the IT Manager of any such emails that are blocked.

Sample Policy 4

(Company name)'s email system exists for the purpose of sending and receiving business information from our customers, suppliers, and stakeholders. We discourage use of the email system for personal business.

Employees must not distribute pornographic (and other offensive or insulting) material and games.

When sending email messages to customers, suppliers, or stakeholders of the company, employees should keep (and file in the appropriate place) a hard copy of the email message and any document or file attached to the message.

Each employee should use the sign-off format that the employee's supervisor considers appropriate.

An audit log of all email messages sent and received by each employee is kept by the system and will be reviewed regularly.

The following message should be added to the end of each email message sent:

This electronic mail message, and any attachment to it, is confidential. If you are not the intended recipient, please reply immediately and destroy the message. You may not copy, disclose, or use this message or its contents. Thank you.

INTERNET POLICIES — SAMPLES

Sample Policy 1

- The internet is to be used primarily for business purposes.

- Personal use: Occasional personal use of the internet is permitted but should be kept to a minimum, as non-work related use will reduce the system's ability to cope with work-related tasks and is a significant cost to the company. *(Company name)* reserves the right to require any user to cease using the internet, either on a temporary or a permanent basis if this privilege is detrimental to the performance of work duties or is abused in any way.

- Correct use: Appropriate examples of business purposes include:
  - information search of a client or supplier website;
  - search for industry updates, trends, etc;
  - downloading of data relevant to (company name)'s business; and
  - support to clients, via appropriate internet access methods.

- Inappropriate use: This includes but is not limited to:
  - downloading or forwarding recreational games, or video or voice files to any company PC or laptop;
  - accessing, downloading, or printing text and graphical information that is offensive, objectionable, or insulting;
  - conducting illegal activities;
  - engaging in activities not related to the business of (company name), including gambling;
  - engaging in any activity that may affect the security of (company name)'s information and business practice;
  - soliciting for personal gain or profit;
  - representing personal opinions as those of (company name); and
  - revealing or publicising proprietary or confidential information.

- Cost of using the internet: *(Company name)* reserves the right to charge for the costs incurred by any user accessing inappropriate sites or using the system for personal reasons.

- Monitoring: *(Company name)* is able to, and will, monitor use of the internet. Audit logs of internet access transactions are recorded and maintained by the company. We may install special software to restrict access if we consider this necessary.

- Breach of this policy: *(Company name)* may take disciplinary action, including dismissal, for any breach of this policy.

Sample Policy 2

Access to the internet will only be allowed if the employee's supervisor believes such access is required for the employee to do his or her job. The internet is to be used for business purposes only. Non-work related use of the internet, eg surfing the internet for entertainment purposes, reduces the system's ability to cope with work-related tasks and is a significant cost to the company. It also increases the risk of computer security breaches and the introduction of viruses to the system.

Employees must not use the internet for any of the following purposes:
- Downloading recreational games, video, or voice files;
- Accessing, downloading, or printing text and graphical information that is offensive, objectionable, or insulting;
- Carrying out unlawful activities or any other activities that might affect the reputation of the company;
- Engaging in business activities not related to the business of the company;
- Engaging in any activity that may affect the security of the computer system;

Each employee's use of the internet will be regularly monitored. An employee's access to the internet may be withdrawn if that employee is found to be using it for personal or other inappropriate use. Further disciplinary action may also be taken, including dismissal in cases of serious abuse of these policies.

Special software has been installed on the computer system to intercept downloaded or emailed files that could affect the capacity and efficiency of the system.

Employees may take part in news groups, chat sessions, and email discussion groups if these sessions are relevant to the employee's work and provided that such participation complies with the other policies set out above.

Sample Policy 3

Staff will be granted internet access if this is required to assist them to do their job. Staff wanting to do an internet search who do not have access may request access to an internet capable computer through management.

Internet usage will be monitored and billed to the department concerned on a monthly basis. Excessive non-work related internet use may lead to the removal of internet access from the staff member(s) concerned. Staff members may not use the internet to download any material that is offensive or that may breach the security or performance/operation of the computer system. Inappropriate usage of the internet may lead to disciplinary action.