**Email, Telephone and Internet Policy**

|  |
| --- |
| Email, Telephone and Internet Policy Sample  This Email, Telephone and Internet template policy s ready to be tailored to your company’s needs and should be considered a starting point for setting up your management policies and processes.  Disclaimer: This policy template is meant to provide general guidelines and should be used as a reference. It may not take into account all relevant local, state or federal laws and is not a legal document. Neither the author nor HR Expert Australia will assume any legal liability that may arise from the use of this policy. |

This policy can only be considered valid when viewed via the [Company Name] intranet site. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one online.

## **Introduction**

This policy explains:

* 1. how you may use email**,** telephones and the Internet using [COMPANY NAME] (The Company’s) facilities;
  2. how you or the Company may be liable in law for misuse of email or the Internet;
  3. how your interests and the Company’s interests can be protected; and
  4. disciplinary action which may be taken against you if you fail to comply with the rules set out in this policy.

1. **General**
   1. You must read this policy and apply it to your everyday work. If you have any questions as to the meaning or effect of this policy you should contact your line manager or a member of the HR Department.
   2. This policy is not a definitive statement of the purposes for which the Company’s facilities must not be used. You must conduct yourself, at all times, in a trustworthy and appropriate manner so as not to discredit or harm the Company or its colleagues and in accordance with the spirit of this policy statement.
   3. This policy applies to all telephone and computer users within [COMPANY NAME] who use email, bulletin boards, intranet, and the Internet, through any computer, accessing company applications or information, via company networks or remotely, whether based at [COMPANY NAME]’s premises or not, or using the Company’s telephone lines.
   4. Failureor refusal to comply with this policy is a disciplinary offence, which may lead to disciplinary action, up to and including, dismissal without notice.
2. **Mobile & Telephone Use**
   1. [COMPANY NAME] funded mobile phone/mobile internet users must, in addition to this policy, also abide by the Company Mobile Phone & Mobile Internet Policy.
   2. The making and receiving of personal calls should be kept to a minimum. When deciding to take or make a personal call, you should use your discretion. You are permitted to use business phones in emergency situations.
   3. You should be aware that mobile telephones can be disrupting and distracting and personal mobile phones should be put on silent, turned off or diverted during working hours.
   4. No land line phone should be forwarded to a mobile phone without the express permission of your direct manager or an equivalent grade of senior management unless deemed necessary. This represents a significant extra cost to the business and must be avoided where it is practical to do so. It is best practice to change the voicemail greeting to advise callers to phone a mobile phone number instead.
3. **Email and Internet**
   1. The Company encourages colleagues to use email as a prompt and effectivemethod of communication. It will not always be appropriate to communicate by email and you should always consider whether there is a more suitable method (for example in circumstances where there is a need to preserve confidentiality or in the case of sensitive issues which should be communicated face to face).
   2. Your use of email and the Internet is only authorised for bona fide purposes directly connected with your work or the Company’s business. All communications and stored information sent, received, created or contained within [COMPANY NAME]’s systems are the property of the Company and accordingly should not be considered as private. As detailed below, the Company reserves the right to access such communications and information.
   3. You must act responsibly and appropriately when using the Company’s computers and when sending email**,** whether internally within the Company or externally using the Internet.
   4. You may only set passwords and security codes for your computer, the system or any part of it or documentation held on it in accordance with Company policy from time to time. The use of someone else’sidentity and password to access the Internet, send email or use any program is strictly forbidden and will result in disciplinary action **unless you are acting in an official capacity by the person concerned and with the permission of your line manager, e.g. PA support**.
   5. You must not deliberately visit, view or download any of the following material and you are strictly prohibited from sending, forwarding, publishing or distributing any material, whether downloaded from the Internet or otherwise which contains or refers to:

* Creation or uploading/downloading of material, which brings [COMPANY NAME] into disrepute;
* Sex or pornography whether illegal material or material comparable to that available on the top shelf in a newsagent;
* Terrorism, Cults;
* Illegal drugs;
* Extreme material which may be likely to cause offence to another person;
* Personal pages;
* Gambling;
* Criminal skills (including software hacking);
* Offensive chat, jokes or chain mail;
* Social networking sites such as Facebook, Bibo, MySpace, Twitter etc;
* Creation or uploading/downloading of material that is illegal;
* The uploading/downloading of unsolicited commercial or advertising material, chain letters, press releases, or other junk-mail of any kind;
* The unauthorised uploading/downloading to a third party of confidential material concerning the activities of [COMPANY NAME];
* The uploading/downloading of material which infringes the copyright of another person, including intellectual property rights;
* Activities that unreasonably waste staff effort or networked resources, or activities that unreasonably serves to deny service to other users;
* Activities that corrupt or destroy other users' data or disrupt the work of other users;
* Unreasonable or excessive personal use. (See Personal Use below);
* Creation or uploading/downloading of any offensive, obscene or indecent images, data or other material;
* Creation or uploading/downloading of material, which is designed or likely to cause annoyance, inconvenience or anxiety;
* Creation or uploading/downloading of material that is abusive or threatening to others, serves to harass or bully others, discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, age, colour, nationality, disability, political or religious beliefs;
* Creation or uploading/downloading of defamatory material or material that includes claims of a deceptive nature;
* Activities that violate the privacy of others or unfairly criticise, misrepresent, including copy distribution to other individuals;
* The unauthorised provision of access to [COMPANY NAME] services and facilities by third parties;
* Downloading music and video content.
  1. You are also strictly prohibited from sending any emails which are:
* threatening or aggressive;
* abusive, anti-social or discriminatory;
* obscene or offensive;
* or have the potential to damage the brand of [COMPANY NAME].
  1. Should you mistakenly locate an Internet site containing any prohibited material (as above)you should notify the line manager and IT helpline so that steps can be taken to avoid other people making the same mistake.
  2. Unauthorised use of email and/or the Internet may expose both you personally and/or the Company to Court proceedings attracting both criminal and civil liability. You will be held responsible for any claims brought against the Company for any legal action to which the Company is, or might be, exposed as a result of your unauthorised use of email and/or the Internet.

### Personal Use

* 1. [COMPANY NAME] permits the use of its IT facilities for email, telephone and internet authorised users for a reasonable level of personal use. An absolute definition of abuse is difficult to achieve but certainly includes (but is not necessarily limited to):
* A level of use that is not detrimental to the main purpose for which the facilities are provided;
* Priority must be given to use of resources for the main purpose for which they are provided;
* Not being of a commercial or profit-making nature, or for any other form of personal financial gain;
* Not be of a nature that competes with [COMPANY NAME] in business;
* Not be connected with any use or application that conflicts with an employee's obligations to [COMPANY NAME] as their employer;
* Not be against [COMPANY NAME] rules, regulations, policies and procedures and in particular this email, telephone and Internet policy.

1. **Software**
   1. [COMPANY NAME] purchases computer licenses and software from a variety of outside sources. The Company does not own this software or related documentation and, unless authorised by the software developer, and does not have the right to reproduce it.
   2. The software used on the local area network or multiple/individual machines should have the appropriate licence(s) and you should only use it according to the licence agreement.
   3. You should notify your manager of any misuse of software or associated documentation.
   4. Should there be the need for any additional software, approval must be granted by a senior or executive manager and then purchased by our IT support system.
2. **Security and Viruses**
   1. The accessibility of the Internet is both an advantage and disadvantage of the system. Whilst you can access a huge amount of information via the Internet, information and emails sent across the Internet may be read by persons unknown to the sender. Potentially anyone could read private and confidential information transmitted on the Internet. Even if some information has been deleted from your screen it may not necessarily be deleted from the Internet system which provides back-up saving mechanisms. Any message or information requiring security or confidentiality should be distributed by an alternative means of communication.
   2. It is vital that you take all necessary steps to safeguard the Company’s computer system from viruses. Accordingly, you must discard any unsolicited documents or attachments which you receive. You must not introduce new software onto the Company’s system without written authorisation from the CEO and you must always ensure that the appropriate virus checking procedures have been followed.
3. **Courtesy**
   1. As emails can easily be misconstrued you must therefore consider very carefully whether email is the appropriate form of communication in particular circumstances. If you decide that it is, you should carefully consider the content of all emails and who the appropriate recipients should be. Pay particular attention to the style and content of all emails when sending externally, treating them in the same way as letters on the [COMPANY NAME] letterhead. All emails should be in line with [COMPANY NAME] style guide and should have a formal signature at the end of each email.
4. **Data Protection**
   1. Only designated colleagues may place colleague information (including photographs) onto the Company’s system. In all cases the individual to whom the personal data relates should have been made aware that this information would be placed on the system. Photographs should not be placed on the system without an individual’s consent. If you are in any doubt you should check with your manager.
5. **Monitoring**
   1. The Company reserves the right, without notice, to access, listen to or read any communication madeor received by you on its computer, mobile telephone, or telephone system for the following purposes:

* to establish the existence of facts;
* to ascertain compliance with regulatory or self regulatory practices and procedures;
* for quality control and colleagues training purposes;
* to prevent or detect crime (including ‘hacking’);
* to intercept for operational purposes, such as protecting against viruses and making routine interceptions such as forwarding emails to correct destinations; or
* tocheck voice mail systems when you are on holiday or on sick leave.
  1. The Company also reserves the right to monitor time spent by colleagues accessing the Internet for browsing. The Company may monitor sites visited, the content viewed or information downloaded where necessary.
  2. The Company also reserves the right to make and keep copies of telephone calls, text messages, or emails and data documenting use of the telephone, email and/or the Internet systems, for the purposes set out above. The Company may bypass any password you set.
  3. Colleagues who require assistance or further explanation of any aspect of this policy should contact their Manager or the Human Resources Department.
  4. Breaches of this policy will lead to disciplinary action. In the event you receive or become aware of obscene, indecent, offensive, inflammatory, discriminatory or socially offensive material you should notify your manager immediately so that appropriate action may be taken.

1. **Incident Handling**
   1. [COMPANY NAME] will investigate complaints received from both internal and external sources, about any unacceptable use of email, Internet, mobiles or telephone that involves [COMPANY NAME] IT facilities. The IT Providers, in conjunction with other departments as appropriate, will be responsible for the collation of information from a technical perspective. Prompt reporting of any incidents which require investigation is recommended.
   2. Where there is evidence of an offence it will be investigated in accordance with [COMPANY NAME] disciplinary procedures applicable to all members of staff. In such cases the IT Providers will act immediately with the priority of preventing any possible continuation of the incident. That is accounts may be closed or email may be blocked to prevent further damage or similar occurring.
2. **Breaches Of Policy**
   1. Users who are found to have breached this policy will be dealt with in accordance with [COMPANY NAME]’s Discipline and Termination policy and, depending on the seriousness of the breach, this may result in instant dismissal.

**Other [COMPANY NAME] Policies relating to this document:**

* Code of Conduct
* Company Mobile Phone & Mobile Internet Policy
* Discipline & Termination Policy