

E-MAIL AND INTERNET POLICY

The key principles of the E-mail and Internet Policy are:

- E-mail (whether internal or external) and internet facilities are for business use and are company property.
- Limited, occasional and lawful personal use in accordance with this Policy is currently permitted.
- Use (business and/or personal) of the e-mail and internet facilities is at the discretion of the Managing Director and may be withdrawn at any time and for any reason.
- Any misuse of e-mail or internet facilities will be taken very seriously. Your use of email and internet facilities must at all times comply with this Policy. Any non-compliant use would result in disciplinary action being taken that could lead to dismissal. If appropriate, relevant authorities (including the police) will be informed.
- Wilcock Consulting reserves the right to monitor the usage and content of e-mail and internet facilities.
- As the law of copyright applies to digital and electronic forms of communication, extreme care should be taken in downloading and circulating third party information. This may involve obtaining the author's consent.
- Everyone employed by or on behalf of Wilcock Consulting must comply with this Policy. "Email and/or internet facilities" are used throughout this Policy to mean the e-mail and/or internet facilities of Wilcock Consulting. "Wilcock Consulting" is used throughout this Policy to mean Wilcock Consultants Limited.

YOU MUST

- Consider whether a face-to-face communication, telephone call or letter is more appropriate than e-mail.
- Ensure that the subject matter of an e-mail is clearly set out in the title field, that the content is clear and concise and that the name and address of the intended recipient is correct.
- Read all earlier messages before forwarding an e-mail message, they may contain comments that will offend.
- Be aware that contracts can be formed by e-mail in the same way as by letter or orally and that an e-mail is likely to be binding on Wilcock Consulting.
- Prepare external e-mails with the same level of care and formality as you would a document on company letterhead. As it is possible for courts to request disclosure of e-mails, do not include anything in an e-mail that you would not wish to be disclosed in court at a later date.
- Consider very carefully who needs to receive the e-mail - do not unnecessarily copy people in.
- When requesting advice from Legal Services by e-mail and you think you may need to protect your request and/or the advice from being disclosed in a court at a later date, you (1) must not send your request or the advice on to anyone other than the lawyer you are dealing with; and (2) must head your E-mail: "For the purposes of seeking legal advice and therefore legally privileged".



- Bear in mind that unencrypted e-mail is not a secure method of communication. Where information is confidential, price sensitive, commercially sensitive or includes personal data, first confirm with your intended recipient that the use of e-mail is an acceptable form of communication
- Remember that all laws governing copyright, defamation, discrimination and contract formation apply to e-mail as well as other forms of written communication.
- Be suspicious if you receive an e-mail/attachment from an unusual source or which contains wording that is either out of context or implausibly attractive.
- Review your e-mails periodically and archive, back up or delete, as appropriate.
- Engage the screen lock facility on your computer when leaving your desks unattended.
- Through your employment with Wilcock Consulting personal data will come into your knowledge, possession or control. In relation to such personal data you must, when using e-mail and internet facilities:
 - Keep them secret and confidential and you must not disclose them to any other person unless authorised to do so by Wilcock Consulting. If unsure contact your line manager
 - Familiarise yourself with the provisions of the Data Protection Act 1998 and its revisions and comply with its provisions
 - Process personal data strictly in accordance with the Data Protection Act 1998 and relevant Wilcock Consulting policies and procedures
 - NOT make personal or other inappropriate remarks about other individuals since the subject of such remarks has a right to see information Wilcock Consulting holds on that individual
 - Be aware that if you make or encourage another person to make an unauthorised disclosure knowingly or recklessly you may be criminally liable

YOU MUST NOT

- Open e-mail attachments from unknown external sources as they may contain viruses. You should alert your supervisor or IT Support Service Provider, (currently Furness Internet).
- Send, save, procure receipt of, distribute, download, display, print, access or view or otherwise disseminate information when using internet and e-mail facilities that is of a racist, pornographic, sexual, obscene, harassing, derogatory, threatening, intimidating, fraudulent, defamatory, or offensive nature. If you are in doubt about a course of action take advice from your line manager.
- Use e-mail or internet facilities for conducting any illegal activities, gambling, or soliciting for personal profit.
- Be over familiar - e-mails do not recognise a sense of humour.
- Infringe any license agreement, copyright, or trade mark law nor download any media or software from a third party website unless the terms of the website specifically authorises users to do so.
- Download application software or programs unless you have explicit authorisation to do so for business reasons.
- Access any information using another employee's password unless explicitly authorised to do so.
- Access any e-mail messages to which you are not the intended recipient (unless you have proxy access).
- Impersonate any other person when using e-mail or maliciously amend any messages received.
- Purchase, order or reserve goods or services on behalf of Wilcock Consulting via the e-mail and internet facilities unless authorised to do so by Wilcock Consulting.
- Overload the system by sending "all user" e-mail messages.
- Produce, introduce or forward chain letters or video clips.
- Send unsolicited junk E-mail (i.e. Spam).
- Expose Wilcock Consulting's information systems to third party software, computer systems or data networks (e.g. the Internet) by circumventing Wilcock Consulting firewall protection.



Wilcock Consultants Limited is an Employment Business
 Wilcock Consultants Limited: Registered in England and Wales No: 2927854.
 Registered Office as above. Registered under the Data Protection Act 1984

- Attempt to disable, defect or circumvent any of the security facilities associated with e-mail or internet usage.

Monitoring

Monitoring of the content and details of recipients and senders of e-mails, and internet sites accessed, may take place where, and to the extent, that Wilcock Consulting is permitted to do so lawfully. You are advised that monitoring may be undertaken for any of the following reasons:

- to ensure compliance with relevant regulations and Wilcock Consulting's policies, procedures and/or standards (including but not limited to this Policy);
- to establish facts, for example to provide evidence of business transactions;
- for training and monitoring standards of service;
- to prevent and detect crime;
- to investigate or detect unauthorised use of the system (for example, breaches of this Policy);
- to ensure the security and/or effective operation of information systems (for example where users have logged a request for e-mail or internet assistance);
- to ensure continued business performance in the event of an employee's absence from work.

Such monitoring may include interception and recording for the above purposes.

To ensure compliance a number of controls are in place to monitor the use of the e-mail and internet facilities. These include:

- electronic scanning of all inbound and outbound e-mails to detect inappropriate images and text in both messages and attachments
- electronic scanning of all inbound e-mails to detect junk email ('spam')
- automatic blocking of e-mails detected as containing viruses or attachments at risk of containing viruses (e.g. exe files)
- access to certain inappropriate categories of internet website is automatically denied

E-mails containing words or images considered inappropriate may be captured and the recipient/sender notified that this has occurred. If the email is business related, and has been stopped in error, the user can arrange for it to be released.

Internet access logs and e-mails logs may be periodically reviewed by management to identify breaches of this Policy.

Disciplinary Procedure

Any misuse of e-mail or internet facilities will be taken very seriously. Your use of email and internet facilities must at all times comply with this Policy. Any non-compliant use would result in disciplinary action being taken. A serious breach of this Policy may amount to gross misconduct and could lead to dismissal. Any suspected misuse of the e-mail and internet facilities should be reported to line management for action as appropriate.

If appropriate, relevant authorities (including the police) will be informed. Unlawful or illegal conduct may be subject to separate criminal or civil proceedings.

Rev 2 May 2010



Wilcock Consultants Limited is an Employment Business
 Wilcock Consultants Limited: Registered in England and Wales No: 2927854.
 Registered Office as above. Registered under the Data Protection Act 1984