

## **Email, internet and IT systems acceptable use policy and procedures**

This policy applies to all thetrainline.com employees. It also applies (except in the case of the disciplinary policy and its sanctions) to third party suppliers and contractors who are given access to thetrainline.com systems. Everyone who has access to any of our electronic communications must comply with this policy. thetrainline.com will take any abuse of Internet and/or email usage or breach of this policy very seriously, which may result in disciplinary action up to and including dismissal. thetrainline.com may pass information to the police to prevent or detect crime.

### **Monitoring**

We keep records of Internet access and email activity carried out on our systems and everything you send or receive by email or through the Internet is company property. Non-business use of thetrainline.com's systems is only permitted on this basis. You should not expect your internet usage at work or personal emails received or sent on company computers to be private.

thetrainline.com has the right to monitor and record information about access and logging on, and email and Internet traffic, as well as actual content. We may do this, for example for security or disciplinary reasons, at any time and without notice. We will not monitor or record the content of telephone calls, email messages or Internet sites visited unless it is clear that the purposes for which the monitoring or recording is undertaken cannot be achieved by other methods.

All email messages are logged and copies recorded in back-up files. Even if you have deleted a message from your in-box, we are still able to find it. Emails may be used in court proceedings and/or investigations by competition authorities and regulatory bodies if relevant. We may have to make your emails available to third parties without your consent at a future date if required by law.

### **Internet Usage**

Our systems (including access to the Internet) are provided for business use. You may use them occasionally for non-business use, but only in accordance with this policy. This includes PCs, laptops, servers, PDA's, WAP enabled mobile phones and any other devices that may be used to access the Internet.

We do not want to stop you using the Internet occasionally for non-business purposes, but you must make sure that it doesn't impact on your work, consume excessive bandwidth, disturb your colleagues or breach the guidelines set out in this policy. Some websites may be restricted by means of content filtering to block access from our network. If you access, forward or store material to which access is not permitted under this policy, you may be subject to formal disciplinary action.

You must ensure that whenever you are online that you:

- use the Internet in a responsible and ethical manner
- use safe and secure web sites
- maintain confidentiality of information
- comply with all applicable legislation and regulatory requirements
- maintain the thetrainline.com brand and reputation

### **Inappropriate usage**

Usage of the Internet is permitted primarily to assist you with your work. When you use the Internet it can consume a lot of our network and system resources especially streaming video and sound files which take up a lot of disk space, computing resources and network bandwidth. You need to bear this in mind when you are online and restrict non-business access to such files.

When you use the Internet at work, whether for business or non-business purposes (including instant messaging and social networking sites), you need to remember that you are using thetrainline.com's systems and network and therefore be responsible and ethical in the web sites that you visit and in the information which you send and receive.

If you are unclear as to what level of non-business usage is acceptable or excessive, you should discuss this with your line manager to obtain clarity.

Do not use the Internet for accessing, uploading, downloading, publishing or transmitting any material which is pornographic, obscene, offensive, racist, discriminatory, homophobic, incites hatred or promotes violence. This includes, but is not limited to:

- sexually explicit messages, images, cartoons or jokes.
- bad language, slander or libel.
- ethnic, religious or racial slurs (which could include images, cartoons or jokes).
- any other material that could be seen as harassing or ridiculing others based on their sex, race, sexual orientation, age, national origin, disability or religious or political beliefs.
- political, terrorist or propaganda material.

You also shouldn't use the Internet for:

- circulating comments about competitors or other colleagues, which are abusive, objectionable or otherwise inappropriate. What amuses you may not necessarily amuse others and may be considered offensive.
- non-business use for long periods, including outside normal business hours. This is a waste of resources, including time, and may affect the way our system performance. This includes using the web for a business that has no connection to thetrainline.com.
- threatening, harassing, propositioning or causing distress, annoyance, needless anxiety or discomfort to anyone else.
- accessing, downloading, forwarding or storing any material that may bring thetrainline.com into disrepute.
- downloading, copying or transmitting to third parties other people's work (including music files) without their permission. You need to keep to the terms of any licences to use copyright material. Always assume that content is subject to copyright unless the owner of that copyright says that you can download, copy or transmit the material.
- downloading software (including games, screensavers, wallpapers etc) unless specifically given permission to do so by the IS support team.
- transmitting any sensitive data such as company or customer's credit card details, passwords or customer account details unless the information has been encrypted and you are authorised to send it.
- posting information about thetrainline.com to public discussion groups (newsgroups), chat rooms, or other public forums on the web, unless you have permission from your manager.
- contributing to or writing Internet Blogs which contain unauthorised company information or opinions.
- signing up to email bulletin boards or newsgroups that require payment from thetrainline.com unless authorised to do so.
- establishing any web pages, electronic bulletin boards, or other mechanisms that provide public access to information about thetrainline.com unless authorised to do so.
- accessing, including browsing, downloading or forwarding material that is in contravention of any applicable legislation and regulatory requirements.
- subscribing to real-time automatic information distribution services (so-called "push services") or to email distribution lists (also known as news groups) unless for legitimate business purposes.
- developing a network connection with a third party (such as an extranet) unless authorised to do so.
- publishing web pages, electronic bulletin boards, or other mechanisms that provide public access to information about thetrainline.com.
- setting up Electronic Data Interchange (EDI) or other electronic business system arrangements.
- making any personal comment outside of thetrainline.com from a thetrainline.com account except where authorised to do so.

- making fraudulent offers of thetrainline.com products, items or services.
- making statements about any warranties or guarantees offered by thetrainline.com unless authorised to do so.
- using the Internet at work for matters relating to a business that is not part of thetrainline.com or is not related to the provision of a thetrainline.com service.

### **Keeping thetrainline.com safe**

The internet is available to anyone and unauthorised individuals can potentially intercept any information you transmit across it. If you transmit confidential or sensitive information in an unprotected manner it may fall into the wrong hands. This could cause damage to thetrainline.com's business operations and reputation, and may lead to negative publicity or even litigation.

Once information is sent outside thetrainline.com's network, you no longer have any control over where that information ends up.

Care must also be taken when entering any information into an external web site. If the information you are dealing with is confidential then you must ensure that the web site is secure. If the web address does not start with *'https://'* it may not be secure service and no confidential information should be entered into it. If you have any doubts, contact the IS support team.

Take care with any information that is downloaded from the Internet. Any files or programs could contain viruses or other malicious programs which could damage and/or disrupt our computer systems and network. You need to ensure that anything you download is safe. Also, some content, such as music files, may be protected by copyright – so ensure that your usage is legal.

### **Email and instant messaging**

Access to email (including instant messaging services) is provided primarily for business use. As such, email must be used in a professional, ethical and responsible manner. In particular, email content must be appropriate, must comply with relevant legal and regulatory requirements and must not cause offence or annoyance. Although non-business use is permitted, individuals need to be mindful that their business email and IP addresses, even when used for non-business purposes, still represents thetrainline.com.

Non-business use of business and personal email and instant messaging systems should be kept to a minimum and must not:

- adversely impact the computing and network resources of thetrainline.com
- affect or interfere with the activity of other employees
- interfere with your ability to perform your normal work duties

You should not use a private email account for work related communications unless you are authorised to do so by your line manager. Please be aware that any work-related communications which are transmitted to or from a private email account remain company property and could be required to be disclosed to third parties by law.

Email and instant messaging can lend itself to hasty, unilateral and informal communication. People tend to be less cautious when writing emails than they would be in preparing other forms of written communications. It is important to remember that email records are permanent (and even after deletion, are retrievable). Emails can also be taken out of context easily. You must be careful not to create emails (or other documents) which could potentially damage the business and/or the thetrainline.com brand.

It is important to remember that emails created at thetrainline.com (or using our systems or network), including from personal email accounts, may have to be disclosed at a later stage in the event of litigation or regulatory investigations. Whilst careless emails may damage the business, carefully prepared email records (for instance evidencing communications or negotiations with third parties) may

help to protect the interests of the business.

There are certain types of email and instant messaging usage which are considered inappropriate when using a thetrainline.com system or account including the following:-

- sending a communication from another user's account without their express authorisation.
- suppressing or replacing your own, or another user's identity on a communication. In all instances your name, electronic mail address and related contact information must reflect the actual originator.
- registering a corporate email address for non business related services.
- non-business use for excessive periods of time, including outside normal business hours. Improper use can lead to a waste of resources, including your time, and may affect the efficient working of thetrainline.com's systems and network.
- use for matters relating to a business that is not in anyway related to your role within thetrainline.com and/or the thetrainline.com business. This includes advertising material or any non-business related material.
- use to exchange any material that may bring the thetrainline.com brand into disrepute.
- entering into any contractual commitments unless explicitly authorised to do so.
- use to receive or exchange content that constitutes an infringement of copyright. E.g. image, music and video files. You need to ensure that you comply with the terms of any licences to use copyright material. You should assume that content is subject to copyright unless the owner of copyright in that work specifically states that you may transmit it.
- creating or forwarding chain email letters.

Do not transmit any communication containing pornographic, obscene, or defamatory material. This includes:

- sexually explicit messages, images, cartoons or jokes.
- profanities, slander or libel.
- ethnic, religious or racial slurs (which could include images, cartoons or jokes).
- any other material that could be construed as harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin, disability or religious or political beliefs.
- political, terrorist or propaganda material.

You must also refrain from:

- circulating comments about competitors or other work colleagues which are abusive, objectionable or otherwise inappropriate.
- sending communications with content that could be considered to be threatening, harassing, propositioning or which could distress, annoyance, needless anxiety or discomfort to any other person.
- sending out sensitive information such as company or third party credit card details, passwords or customer account details.
- entering into contractual agreements without authorisation.
- transmitting or causing the transmission of mail bombs, chain letters or pyramid schemes.

#### **Receipt of inappropriate or offensive content**

If you receive any unacceptable material by email (whether content from inappropriate websites or emails which could themselves cause offence or annoyance):

- do not enter into any dialogue with the sender
- keep any emails that you have received – do not delete them
- do not forward the emails to anyone else
- immediately inform Human Resources

Human Resources may require you to send them the offensive emails as attachments and they will be able to give you instructions on how to do this. Doing so will not put you in breach of this policy.

### **SPAM email**

From time to time, you may receive what is known as 'SPAM' email. SPAM email is invasive Internet advertising and is usually sent from an email account that you do not recognise. The email is normally for commercial purposes from companies trying to sell products and/or services, a number of which are 'scams'. It is typically sent by automated means.

Large quantities of SPAM email can have a detrimental effect on the performance of our systems and network because it consumes space, bandwidth and resources. We have tools and systems in place to help reduce the levels of SPAM.

A lot of SPAM email comes with an invitation to 'remove' yourself from the mailing list - don't. By replying to SPAM email you are confirming your email address and you will almost certainly receive even more SPAM email. Likewise you should never forward unsolicited bulk email advertisements or commercial messages.

Never reply to or open any spam e-Mail. If you receive SPAM e-mail contact the IS support team who can advise you on how to block any more such e-mails from being received.

### **Security considerations**

Email attachments can contain 'malware' which are malicious programs which can infect thetrainline.com's computer systems and network causing disruption and/or damage. When you click on the email attachment the programs become active and cause damage. Do not open any email attachments unless you are aware of the content and sender.

thetrainline.com has confidential and/or sensitive information on our systems, for instance information about our customers and/or colleagues. Information such as bank details, credit/debit card details, National Insurance numbers, confidential product information, and other sensitive information are all contained in our systems.

You must ensure that all confidential and sensitive information that you transmit across the Internet is protected by secure passwords or encrypted. You should also check, before sending any confidential or sensitive information externally, that you have authority to do so. If in doubt, you should seek approval from your line manager.