

STRATHCLYDE
FIRE & RESCUE



THE BOARD OF STRATHCLYDE FIRE & RESCUE

Information Security

Interim Usage Policy for IT Systems

April 2009

STRATEGIC PLANNING DIRECTORATE



Version Control

Version No.	Date	Changes
1.0	17/09/2008	First issue
1.1	10/03/2009	Second issue

Table of Contents

1. Introduction	4
1.1. Applicability	4
1.2. Non compliance with policy	4
1.3. Policy Principles	4
2. Use of e-mail	4
4. Mobile Equipment	6
5. Good Security Practice:.....	7

1. Introduction

1.1. Applicability

This policy is applicable to all staff, contractors and third parties employed by Strathclyde Fire and Rescue and it provides guidance on acceptable standards for using IT equipment throughout the organisation and equally when accessing SFR systems remotely where authorised.

1.2. Non compliance with policy

Indications of non-compliance with the provisions of this policy shall be investigated in accordance with the Strathclyde Fire and Rescue's disciplinary procedures.

1.3. Policy Principles

Strathclyde Fire and Rescue has deployed systems and services to allow it to carry out business objectives in line with its overall business plan. These facilities are designed solely for lawful undertakings of the organisation and not for personal, unlawful or otherwise inappropriate purposes. Specifically, systems and services must not be used:

- For personal gain or profit
- To provide information about employees to persons or businesses not authorized to possess that information
- When it interferes with your job or the jobs of other employees
- When it interferes with the rights of others
- When it might endanger or otherwise put at risk another individual

2. Use of e-mail

E-mails sent from an organisation have the same weight in law as though they were sent to the recipient on headed notepaper. Care should therefore be taken when composing e-mails to avoid:

- Creating unintended contractual agreements through acceptance or acknowledgement of another party's offer or conditions
- Distributing unlawful, offensive or inappropriate material for which the organisation would be held responsible and could be prosecuted
- Transmission of unsolicited, commercial or advertising material, chain letters or junk mail of any kind
- Unauthorised transmission to a third party of sensitive information concerning the activities of Strathclyde Fire and Rescue. Unencrypted e-mails sent outside the organisation can be easily intercepted and read by someone with basic equipment and technical knowledge. Sensitive information should not be sent by outside the organisation by e-mail unless encrypted.
- Transmission of material such that this infringes the copyright of another person, including intellectual property rights

- Unauthorised provision of Strathclyde Fire and Rescue services and facilities by third parties
- Activities that waste staff effort or networked resources or activities that deny service to others e.g. sending large attachments to numerous recipients
- Transmission of obscene, offensive or indecent images or data
- Creation or transmission of material that discriminates or encourages discrimination on social, ethnic, gender, sexual orientation, marital status, disability and religious or political beliefs
- Creation or transmission of defamatory material that includes claims of a deceptive nature
- Criticising individuals, including copy distribution to other individuals
- Publishing to others the text of messages written in confidence without express consent of the author
- Transmission of any message that could bring Strathclyde Fire and Rescue into disrepute

Remember that what might seem like a harmless comment in a face to face situation may appear to be offensive in an e-mail since the recipient has no eye contact with which to judge the tone of the comment.

- Personnel should consider if using the phone is a more appropriate means of communication
- Emails are not confidential and can be read by anyone given a degree of expertise
- Emails should be regarded as published material

Strathclyde Fire and Rescue reserves the right to sample or scan e-mail traffic to monitor its use for appropriate content.

3. Internet use

Strathclyde Fire and Rescue provides Internet access for business purposes only. However, occasional personal use of the Internet facility will be permitted provided that it is not abused and complies with other rules in this policy.

You must not access, browse, create, upload or download unlawful or offensive material. Specifically, you must not:

- Knowingly violate any laws or regulations. Strathclyde Fire and Rescue will co-operate with any legitimate law enforcement agency in bringing people to justice.
- Knowingly download or distribute pirated software or data
- Deliberately introduce or pass on any virus or other type of malicious code
- Download entertainment software or games or play against opponents across the Internet
- Download images or videos unless there is a specific business related use for the material
- Download audio files such as MP3, WAV, OGG etc. unless for business use
- Download streaming media such as Internet radio stations

Strathclyde Fire and Security reserves the right to monitor Internet usage for content.

4. Mobile Equipment

Users of mobile equipment such as Laptops and PDAs are responsible for their security and ensuring the security of any data held thereon.

- Always ensure mobile equipment not being used is stored out of site.
- Take steps to avoid being seen by others when, for example, stowing equipment in the car boot. Thieves often wait around motorway service areas watching for equipment being stowed in the boots of cars.
- When staying in hotels make sure portable equipment is stored securely
- Laptops left in the office overnight should be stored securely in lockable cupboards or drawers.
- Where possible, information held on portable devices should be encrypted, particularly if it is sensitive. Where equipment holds sensitive data it should not be left attended at any time
- Always use security features provided including password protection

- Report any loss mobile equipment immediately to the Police and the IT department.

5. Good Security Practice:

- Passwords must be kept safe and not divulged to anyone else either inside or outside the organisation. Do not use passwords that can be easily guessed such as your child or partner's name. Use strong passwords that include a mixture of upper, and lower case, special characters and numbers. If you need further advice on how to do this contact the Helpdesk.
- Work-stations (including laptops) will be set up to provide users with appropriate levels of access. Do not access or attempt to access parts of the system that would require additional access rights. Never attempt to gain access to a system by using another person's UserId and Password.
- Always lock your work-station when leaving your desk. If you need further advice on how to do this contact a member of the IT department.
- The Information Systems are protected against viruses and other malware attacks by a comprehensive set of tools that are routinely maintained. You must not interfere with these tools, for example by attempting to disable the anti-virus software on your desktop.
- Information arriving into the organisation through the gateways (either by Internet or e-mail) is routinely scanned to ensure that it is free from viruses and malware. All removable media including CD, DVD, USB data sticks containing information to be transferred to the network must be scanned before attempting to connect to the network.
- Any stand alone equipment, not routinely connected to the network, will not be protected against virus attack. You must make alternative arrangements to protect any information contained thereon by contacting the IT department.
- Where laptops or PDAs are being used outside the organisation to connect to wireless hotspots at airports etc. then special care must be taken to ensure viruses are not imported through these connections. Important or sensitive information should not be transmitted through wireless connections unless an appropriate level of encryption has been established as part of the connection. If you need further advice on encryption you should contact the Helpdesk.

Glossary

MP3	Digital audio encoding format
WAV	Waveform Audio Format
OGG	Open source Audio File Format
DVD	"Digital Versatile Disc" or "Digital Video Disc"
USB	Universal Series Bus

PDA Personal Digital Assistant

Userld User Identification or logon name e.g. BloggsJ