

BEDFORDSHIRE AND LUTON FIRE AND RESCUE SERVICE

INFORMATION SECURITY POLICY STATEMENT - POLICY ON THE USE OF THE INTERNET

Reference: Information Security Policy Statement V1 7 dated 28 Sep 2001

1 Introduction

Bedfordshire & Luton Combined Fire Authority has provided networked access across all Service sites and to the Internet to help the staff do their jobs more efficiently and effectively. Access to the Internet makes available the vast information resources of the World Wide Web (WWW) and provides the capability to communicate beyond the environs of the Service using Internet e-mail. However, these opportunities also bring risks of compromise and damage to the confidentiality, integrity and availability of Service information (for example from computer hackers). Additionally, because of the vast range of information on the web there is the possibility that staff time may not be used effectively, and access to information from undesirable sites could lead to damage to the reputation of the Service or even criminal prosecutions.

This document explains the Service's policies for use of the Internet, which is underpinned by the premise that it has been provided for business use, to communicate with citizens, customers and suppliers, to research relevant topics and obtain useful work-related information, and to assist in the development of employees.

Internet web sites, discussion groups and email give each individual Internet user the unprecedented capability to propagate corporate Service information. Because of that power, users must take special care to maintain the clarity, consistency and integrity of the Service's corporate image. For instance anything any one employee writes in the course of acting for the Service on the Internet could be taken as representing the Service's corporate position. It is therefore important that staff conduct themselves honestly and appropriately on the Internet, and respect the copyrights, software licensing rules, property rights, privacy and prerogatives of others, just as one would in any other business dealings.

For the reasons outlined above all Service employees applying for Internet access are required to sign the 'Internet Code of Conduct' prior to use; however, if individuals are not willing to sign, Internet facilities will not be granted. The 'Internet Code of Conduct' itself is based on the policy statements expressed within this document.

2 Applicability

The policy covers both use of the WWW and use of Internet e-mail as described below and applies to all employees of the Service, (whether permanent staff, agency or temporary staff), and any other organisations or individuals using Service IT facilities.

3 Authorisation

Access to the Internet will be granted only where there is a business need, and additional costs (if any) are provided for in budget funds. Internet facilities should be applied for using the Form FSIT 1 (Request for External E-mail and/or Internet Access). Staff will also be required to sign and return the Internet Code of Conduct, Form FSIT 2, before access will be given.

Both the forms should be returned through the responsible Line Managers, using the distribution list on the FSIT 1. The completed Code of Conduct will be filed on an individual's personal folder in the Personnel Section and a copy returned to the originator.

Misuse of the Internet may lead to the facility being withdrawn from that individual.

4 Internet Policy Provision

4.1 Prohibited Activity

Employees are not to access any material that might be considered offensive, inappropriate or may adversely affect the reputation of the Service. This includes racist and sexist information, pornographic material, and sites promoting violence, offensive language and unlawful conduct. However, it is possible to access undesirable sites by accident, such connections should be broken immediately, and the incident reported to the responsible Line Manager so that the Service will know of genuine accidental accesses of such sites. The Line Manager in turn must report the event to the IT Manager so that access to the site can be blocked.

The display of any kind of sexually explicit image or document on any Service system is a violation of Service policy on Dignity at Work and is prohibited. In addition, sexually explicit material may not knowingly be accessed, archived, stored, distributed, edited or recorded using the Service's network or computing resources.

Individuals must not use the Internet for private business purposes, for party political purposes or on-line gambling.

The Service's Internet facilities and computing resources must not knowingly be used to break the law. Use of any Service resources for illegal activity is grounds for immediate dismissal, and the Service will co-operate with any legitimate law enforcement activity. Illegal activities include accessing certain categories of sites, typically associated with paedophilic images, activities constituting 'hacking', and illegal copying of software. The Copyright, Designs and Patent Act, Computer Misuse Act, Data Protection Act and laws of libel are all applicable to activities over the Internet. Individuals should assume that all materials on the Internet are copyrighted unless specific notice states otherwise.

Employees with Internet access are not permitted to download any software. Where software is required from the Internet and is for business use, arrangements are to be made for the proper procurement of the software through the IT Manager.

No employee may use Service facilities knowingly to download or distribute pirated software or data.

No employee may use the Service's Internet facilities to deliberately propagate any anti-security or other damage inducing software such as a virus, worm, Trojan horse, or trap-door program code.

No employee may use the Service's Internet facilities knowingly to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.

Use of Service Internet access facilities to commit acts such as misuse of Service assets or resources, sexual harassment, unauthorised public speaking and misappropriation or theft of intellectual property are prohibited.

Employees with Internet access may not use Service Internet facilities to download entertainment software or games, or to play games over the Internet.

Employees with Internet access may not use Service Internet facilities specifically to request the downloading of high capacity images (over 10 MB) or videos unless there is a specific business-related use for the material.

Employees with Internet access may not upload any software licensed to the Service or data owned or licensed by the Service without explicit written authorisation from the IT Manager.

4.2 Control of Information

All Service Groups/Teams/Stations and partner organisations are required to observe the relevant provisions of the Data Protection Act and to conform to the Service's policies and procedures relating to data protection and security. In this respect, material classified under the HMG Protective Marking Scheme (PMS), or containing sensitive or confidential Service information must not be transferred over the Internet, by email or any other means unless encryption is used. This restriction also applies to such information as telephone calling card numbers, log-in passwords, security parameters that could be used to gain access to goods or services and credit cards, except when used to purchase goods and services on a secure site which uses SSL encryption.

Individuals shall not disclose on the Internet, internal Bedfordshire & Luton Combined Fire Authority information that is likely to adversely affect the reputation of the Service, customer relations, or public image. However, official responses by individuals in the course of their duties, to specific electronic mail messages and communications for professional purposes with recognised professional bodies are permitted.

It is relatively easy to falsely assume the identity of another user on the Internet; therefore the release of any internal Service information, entering into any contracts, or ordering of any products is prohibited, except on authenticated e-commerce sites.

The Service retains the copyright to any original material posted to any forum, newsgroup, chat or WWW page by any employee in the course of his or her duties.

4.3 Public Forums

Chat-rooms and newsgroups are public forums where it is inappropriate to reveal official Service information, customer data, trade secrets, and any other material covered by existing Service confidentiality policies and procedures. The release of official information via a newsgroup or chat-room is prohibited.

It is Service policy not to provide access to newsgroups and the system has not been set up to provide these facilities. This policy has been made on the basis that newsgroups are transient in nature and it is therefore not possible to filter out the substantial number of highly undesirable sites that exist on the Internet in any effective way.

Each employee using the Service Internet shall identify himself or herself honestly, accurately and completely (including their Service affiliation and function where requested) when participating in chat-rooms, or when setting up accounts on outside computer systems. Misrepresenting, obscuring, suppressing, or replacing a user's identity on the Service Internet, or in any Bedfordshire & Luton Combined Fire Authority electronic communications, is forbidden. The user name, electronic mail address, organisational affiliation, and related information included with messages or postings must reflect the actual originator of the messages or postings.

Only those employees or officials who are duly authorised to speak to the media or in public gatherings on behalf of the Service may speak/write in the name of the Service to any chat-room or newsgroup. Other employees may participate in chats in the course of business when relevant to their duties, but they do so as individuals speaking only for themselves. Where an individual participant is identified as an employee or agent of this Service, the employee must refrain from any unauthorised political advocacy and must refrain from the unauthorised endorsement or appearance of endorsement by the Service of any product or service. Only those managers and Service officials who are authorised to speak to the media or in public gatherings on behalf of the service may grant such authority to chat room participants.

4.4 Personal Use

Bedfordshire & Luton Combined Fire Authority recognises that the Internet is an invaluable resource for the provision of information, research and communication. Therefore, personal use by authorised users is permitted, provided the use is not contrary to the Service's interests, this policy, or the Internet Code of Conduct and it is done in personal time and not Service time.

Personal use includes private study and research linked to recognised professional development, hobbies and interests, and as a general information resource. Users are advised that the Internet is inherently insecure and that there is no guarantee that personal and sensitive information can be kept private. Personal information should not be stored on terminals or PCs.

4.5 Good Practice

Where possible communications which include intensive operations such as large file transfers, mass e-mailing and the like should be scheduled for off-peak times, (ie outside the hours of 0900 - 1700 Monday to Friday).

Video and audio streaming and downloading technologies represent significant data traffic which can cause local network congestion. Video and audio downloading is therefore prohibited without the explicit authorisation of the IT Manager.

Intentional automatic updating of software or information onto Bedfordshire & Luton Combined Fire Authority computers via background 'push' Internet technology is prohibited unless the involved vendor's system has first been tested and approved by the IT Manager. While powerful and useful, this new technology could be used to spread viruses, and cause other operational problems such as system unavailability.

Employees may not establish Internet web sites or pages, dealing with Bedfordshire & Luton Combined Fire Authority business, or make modifications to existing web pages, unless they are designated, authorised information managers for specific information pages. Modifications include the addition of hot-links to other sites, updating the information displayed, and altering the graphic layout of a page.

4.6 Security and Audit

Computers that use their own modems to create independent data connections circumvent network security mechanisms; therefore, any computer used for independent dial-up or leased-line connections to any outside computer or network must be physically isolated from the Service's internal networks.

The Service has installed a firewall as an essential facility to assure the safety and security of the Service's data and networks. Additionally, software to identify a whole range of inappropriate, dedicated leisure, or sexually-explicit Internet sites will be used to block access from within the network to all such sites that are known to the software.

The Internet gateway is capable of monitoring and recording the time spent on the Internet by each and every user, and the usage data may be used to check that Service Internet resources are properly applied to maintaining the highest levels of productivity during working hours.

Any file that is uploaded or downloaded will be scanned for viruses centrally through the use of memory resident or network virus checking software. As a precaution, any file received must be checked for authenticity by the end user before opening and the IT Manager consulted if there is any doubt as to its source or nature.

Connections to the Internet will be automatically disconnected after a period of inactivity, to prevent unauthorised use of machines that have been inadvertently left logged on.

User IDs and passwords help maintain individual security and accountability for Internet usage. Any employee who obtains a password or ID for the Internet must keep that password confidential. The sharing of user IDs or passwords obtained for access to Internet sites is prohibited.

Employees shall not probe security mechanisms at either Bedfordshire & Luton Combined Fire Authority or other Internet sites. Attempts to probe security mechanisms will trigger alarms, and resources will needlessly be spent tracking the activity. The possession of tools for cracking information security is prohibited. The periodic testing of security systems will only be undertaken with the authorisation of the IT Manager.

Employees must not attempt to disable, defeat or circumvent any Service security facility.

5 Internet E-Mail Policy

5.1 Management Arrangements

All the above policy statements are also applicable to Internet E-mail and are modified or added to by this section.

5.2 Security

To protect the Service system, all incoming e-mail will be checked automatically for malicious code; additionally, automatic text scanning will check for offensive words and phrases and for patterns which indicate unsolicited mail (spam). Any mail containing high risk material will be quarantined and the originator notified of the action taken. Where an individual receives inappropriate material by e-mail, he/she must report the circumstances immediately to their Line Manager and the IT Manager, so that action to prevent a recurrence can be taken.

Partner organisations and others wishing to make use of the Service's e-mail facilities will be required to agree in writing to observe this policy or one agreed by the Service as equally acceptable.

5.3 Acceptable Use

Use of e-mail must be consistent with individual staff's normal responsibilities and should comply with all other rules and procedures relating to communication.

The use of e-mail must conform to all the relevant Service policies including those on sexual and racial harassment and abuse.

The use of obscene, abusive or sexually explicit language or images, is not acceptable, nor is the use of e-mail to transfer illegal, lewd or offensive material into, across or out of the Service system.

Employees are not to use corporate resources, including electronic communications to create either the appearance or reality of inappropriate use.

E-mail, even inside the Service, is a form of publication. Individual employees as well as the Service are potentially liable to action for libel, defamation or breach of trust. E-mail must not be used for potentially libellous or defamatory purposes. To avoid libel, defamation of character, and other legal problems, derogatory comments or written attacks are prohibited.

Employees must not make threats against another user or organisation and all e-mail messages intended to harass, annoy, or alarm another person are prohibited.

Retained e-mail documents may have to be disclosed to individuals or outside agencies in legal cases, as required by current litigation, Data Protection and Freedom of Information legislation.

The Service's policies on communications with the media or appearing to act as a spokesperson for the Service apply also to e-mail communications.

5.4 Personal

Bedfordshire & Luton Combined Fire Authority recognises that the Internet provides a ready means of sending cost-free messages to distant individuals in a social capacity. However, the Service e-mail should not be relied on for important personal transactions, or as your sole personal email address as the Service has the right to terminate or change the facility to support its operational and business needs. Additionally all email entering or contained on the system may be accessed for legitimate Service reasons. Limited use of email for personal purposes is therefore allowed, provided:

- it is done in personal time and not Service time,
- personal e-mails are marked 'Personal' in the subject heading,
- no business activity is pre-empted by personal use,
- it does not consume more than a trivial amount of resources,
- it does not interfere with business activity.

On the last point employees shall not use the Internet or other internal information systems in such a way that the productivity of other employees or the systems is eroded; examples include chain letters and broadcast charitable solicitations, or the sending of bulk e-mails apart from those that are to support the business functions of the Service. A work e-mail address is not to be used to register on any web site for personal purposes such as shopping, trading or mail shots.

5.5 Disciplinary Measures

Abuse of the Internet facilities or violation of this policy will be fully investigated using the Disciplinary Procedures applicable to uniformed and non-uniformed staff.

6 **Application Forms**

Form FSIT 1 Request for External e-mail and Internet Access
Form FSIT 2 Code of Conduct Certificate

ISM/SN

Route:
Applicant
Line Manager
Information Security Officer (ISM)
IT Manager
IT Technical Officer

FSIT 1
 (16.6.05)

**BEDFORDSHIRE AND LUTON FIRE AND RESCUE SERVICE
 REQUEST FOR EXTERNAL E-MAIL &/OR INTERNET ACCESS**

NAME OF APPLICANT	
GROUP	
WATCH/SECTION	

Business case: (Specify why you need access, indicating web sites to be visited and external e-mail addresses or organisations which will be contacted).

Applicant's Signature		Date	
----------------------------------	--	-------------	--

Direct Line Manager's Comments: (Recommendation)

Signature		Name		Date	
------------------	--	-------------	--	-------------	--

Second Line Manager's Comments (To approve the business case)

Approved		Not Approved	
-----------------	--	---------------------	--

Signature		Name		Date	
------------------	--	-------------	--	-------------	--

Information Security Officers (ISM) Comments:

Signature		Date	
------------------	--	-------------	--

IT Managers Comments:

Approved		Not Approved	
-----------------	--	---------------------	--

Signature		Date	
------------------	--	-------------	--

To be completed by the IT Tech Officer:

Authorised by line manager
 Authorised by InfoSecO
 Authorised by ITM
 Internet Code of Conduct completed
 Name added to Internet user register
 Signed Internet Code of Conduct passed to personnel
 Date & time access granted

Signature		Date	
------------------	--	-------------	--

CODE OF CONDUCT

(This form must be read, signed and returned before staff can access the Internet)

I have received the approval of my line manager and/or a senior manager for the use of the Internet facilities as part of my work for the Service.

I have read in full the Service's Internet Usage Policy and have received clarification on any areas that were not clear to me. I understand that the Internet is to be used in order to support the operations of the service, usually during normal working hours. I also understand that outside working hours, the Internet may be accessed, where required in order to perform research linked to recognised professional development and for casual use for hobby or general interest purposes provided this is in no way contrary to the interests of the Service.

I will ensure that I do not transfer material classified under the HMG Protective Marking Scheme (PMS), or subject to the Data Protection Act over the Internet, by email or any other means.

I will ensure that I do not knowingly infringe any copyright restrictions on materials accessed or transmitted via the Internet, nor use email or internet facilities for illegal purposes.

I will avoid deliberately accessing any material that might be considered offensive or inappropriate. This includes all racist and sexist information, together with any material that might be considered to be pornographic. It also includes sites promoting violence, offensive language and unlawful conduct. I will report any accidental accessing of offensive material to my line manager and the IT Manager.

I will ensure that files downloaded from the Internet or received by email will be checked for authenticity before being used, if the source is unknown immediate action will be taken to deal with it by contacting the IT section.

I will ensure, that my emails do not contain materials or language which are lewd or offensive, or that are defamatory or libellous in nature and, could result in legal action being taken against me.

I will not send bulk emails apart from those which may be considered to be essential to support the functions of the Service.

I will not allow access to the Internet facility to unauthorised personnel.

I understand that my time on the Internet is recorded and that the information may be used to check on and measure the usage patterns of the Service Internet facility.

I understand that abuse of Internet facilities will be investigated under the provisions of the Disciplinary Procedures applicable to uniformed and non-uniformed staff. Some abuse could be viewed as acts of Gross Misconduct and could lead to dismissal and/or criminal proceedings.

By signing below I confirm that I have read and understood the Service Policy on the Use of the Internet and I have read and accepted the above Code of Conduct for use of the Service's Internet facilities.

Name: Post:

Department or Section:..... Signed:..... Date:.....

Actioned by IT: Name:..... Signed:..... Date:.....