



Highlands & Islands Fire & Rescue Service

INTERNET, E-MAIL AND TELEPHONE ACCEPTABLE USAGE POLICY

1. Policy Statement

HIFRS will ensure that the use of all IT facilities are made in compliance with all appropriate legislation eg Data Protection Act (DPA), Freedom of Information (Scotland) Act (FOISA), Computer Misuse Act (CMA) and the Regulation of Investigatory Powers Act (RIPA).

2. Purpose of the Policy

The purpose of this policy is to ensure that HIFRS is compliant with all appropriate legislation and all users of the Service's Computer Systems, Networks and Telephones are aware of what is acceptable and unacceptable usage.

3. Scope & Responsibility

This policy applies to all aspects of computer systems, networks, telephones and radios supplied by or on behalf of the Service.

This policy applies to **all** Service employees, and any other persons permitted to use Highlands and Islands Fire and Rescue Service (HIFRS) Information Technology (IT) facilities.

The Area Manager for Operations Support is responsible for the implementation and compliance of this policy.

4. Implementation of Policy

This policy is effective from **31 March 2009** and all staff should refer to the Acceptable Usage – Internet, E-mail and Telephone Procedure to ensure this policy is complied with.

5. Definitions

IT facilities are defined as computer systems, computer hardware and software, networks, telephones and radios.

6. Expectation of Proper Conduct

All users will be notified of the Acceptable Use Policy to which these guidelines refer, via a logon screen which will appear whenever a user logs-on. To proceed, users will have to click on a button that states "**By clicking here I accept all Service policies on the use of computers, including e-mail and the Internet**".

In addition, all such policies and guidelines will be available on-line. Further, new employees should not be given access to e-mail or the Internet until they have seen and accepted these policies. This will be the responsibility of their line manager in respect to the Induction checklist issued on the new starter's arrival.

7. Communication Policy

Effective communication is vital to increase staff awareness of these guidelines and their use within the services.

Any major revisions to this policy will be notified via e-mail, where appropriate.

8. Requirement to Comply with Legislation

The use of all IT facilities must be made in compliance with all appropriate legislation e.g.

- Data Protection Act (DPA),
- Freedom of Information Act (FOI),
- Computer Misuse Act (CMA)
- Regulation of Investigatory Powers Act (RIPA).

9. Requirement to Conform with all Service Policies

The use of all IT facilities must be made in compliance with all Service policies e.g. Information Security Management System, Policy and Manual, Fairness at Work Policy.

10. Consequences of Failure to Comply with Legislation or Policies

If a user fails to comply with any legislation or policy, including any of the acceptable use provisions outlined in this document, use of the system may be withdrawn and future access may be restricted or denied. This may impact on the individual's ability to undertake the duties of their job.

Some violations may also constitute a criminal offence and result in legal action. Any user violating these provisions, applicable national laws, or Service policies, is subject to loss of access privileges and any other legal or Service disciplinary procedures.

11. **Monitoring Usage and Access to Systems**

The Service reserves the right to monitor, log and access all computer, telephone and network activity including Internet access and E-mail, with or without notice. Users should, therefore, have no expectations of privacy in the use of these systems.

The Service has 3rd party "firewall" software and systems in place to monitor all Internet usage and these will be checked and analysed on a regular basis. Sites will be blocked if they are deemed to hold inappropriate or sexually explicit material. A record of site access is retained for a minimum of 3 months. IT staff will investigate any issues exposed which may involve individual user's activities.

Although the Service respects the privacy of every individual throughout the organisation, all E-mail will be checked for content and attachments to ensure that at all times the security and integrity of the Service is not impeded. The sender of any message that is intercepted will be recorded. A record of all E-mail is retained for a period of 6 months.

12. **Acceptable Use**

The following criteria will be used to assess whether usage is acceptable:

- Be in support of business and service needs consistent with Service policies
- Be in support of an individual's approved duties
- Be consistent with the regulations appropriate to any system or network being used /accessed
- May be for limited personal usage provided this is not associated with personal gain or monetary reward, is not interfering with the delivery of Service objectives, does not violate this or any other Service policy and is a lawful activity

13. **Unacceptable Use**

It is unacceptable for a user to use, submit, publish, display, download or transmit on or from the network, telephone or on any computer system any information which:

- Violates or infringes on the rights of any other person, including the right to privacy
- Contains defamatory, abusive, obscene, pornographic, profane, sexually orientated, threatening, racially offensive, or otherwise biased, discriminatory, or illegal material
- Violates Service regulations prohibiting personal harassment
- Restricts or inhibits other users from using the system or the efficiency of the computer systems by excessive downloading or streaming of on-line radio/audio or video. As stated earlier, the Service reserves the right to monitor Internet and E-mail use. It is unacceptable for users to misuse the facilities
- Encourages the use of controlled substances or uses the system for the purpose of criminal intent; or
- Uses the system for any other illegal purpose
- Is used to conduct any non-approved business
- Is used to transmit material, information, or software in violation of any local or national law

SECURITY CLASSIFICATION: **NOT PROTECTIVELY MARKED**

- Is used to copy material which is protected by copyright laws, such as MP3 music, video, films or books.
- Is used to access or transmit information via the Internet, including e-mail, which is not acceptable to the Service; (e.g. Spyware, Junk Mail, Chain Letters etc)
- Is used to access or transmit information via Internet, including e-mail, in an attempt to impersonate another individual; (e.g. Spoofing)
- Is used to conduct any other unauthorised activity (e.g. Gambling).

Clarification of any of the above acceptable and unacceptable uses should be sought from the line manager or the I.T./ Comms manager.

Should users indulge in unacceptable use as defined above they may be subject to disciplinary action under the Service's Disciplinary Procedures. In certain cases this may amount to gross misconduct e.g. accessing pornographic or obscene material which would normally lead to summary dismissal, subject to normal Disciplinary Procedures.

14. **Security**

Access and usage of systems must be in accordance with the Service's Information Systems Security Policy.

- Users must not reveal their account password or allow another person to use their account
- Users must not use another individual's account
- Users must not attempt to log on as another user
- Users must notify the Service Desk immediately if they identify a security problem
- Users must not show or identify a security problem to others
- Users must take reasonable precautions to protect the Service's systems from security issues such as computer viruses
- Use only properly supplied and authorised systems for undertaking Service business.
- Any user identified as having a history of problems with other computer systems may be denied access
- Users should use only the recommended software to access the Internet.

15. **Remote Access**

Remote access is provided within the service network to allow users and contractors to access the Services network and resources for approved tasks.

16. **Etiquette**

When using IT facilities users must:-

- Be polite
- Not use vulgar or obscene language
- Use caution when revealing personal information such as their address or phone number or sensitive information about other people, including staff in confidence information.

SECURITY CLASSIFICATION: **NOT PROTECTIVELY MARKED**

- Use caution when revealing their address or phone number (or those of others)
- Be aware electronic mail is not guaranteed to be private
- Not intentionally disrupt the network or other users
- Abide by generally accepted rules of network etiquette.

17. **Internet**

17.1 **Purpose of the Internet**

The Internet (including external E-mail) is a global communications network which provides vast, diverse and unique resources. With access to computers and to people all over the world users can gain access to material that may not be considered to be of value to the Service. There may be some material or individual communications that are not suitable for everyone. The Service views information gathered from the Internet in the same manner as reference materials identified by the staff. Specifically, the Service supports resources that will enhance the business and service environment. Exploration and manipulation of resources is encouraged where this benefits the Service and staff development within their post. However, it is impossible to control all materials on a global network and users may discover inappropriate information.

17.2 **Access to the internet**

Access to the Internet and use of internal and external E-mail, is provided as part of the standard Office Service which is provided on every desktop system and is available through normal levels of authorisation (usually via line managers). Only hardware and software supplied in accordance with the Service policy is acceptable for Internet & E-mail access.

17.3 **Virus protection**

To prevent the risk of potential viruses, users should not open any unsolicited e-mail attachments or independently load any software, including screensavers, onto their computers. If a user does inadvertently open a message or attachment that contains a virus, they need to contact the I.T. Helpdesk immediately and close the message and attachment. It should not be accessed again without approval from the I.T. Helpdesk.

17.4 **Filtering and Access to Inappropriate Material**

Access to the Internet via the Service's systems is "filtered". The intention is to prevent access to certain sites, for example, those containing pornography. The system, however, is not fail-safe and the Service cannot prevent the possibility that some users may access material that is not consistent with the policies of the Service, or in line with the employee's normal duties and responsibilities. Where material, which is not consistent with the policies of the Service, is inadvertently accessed, people are strongly advised in their own interest to report the matter to their line manager. If there is any doubt as to what constitutes inappropriate material, the user should seek advice from the line manager or the IT/Comms Manager. If a user continues to access inappropriate material this will be treated as unacceptable access as per Section 13.

17.5 Accuracy and Quality of Information

The Service will not be responsible for the accuracy or quality of information obtained through its Internet connection.

18. E-mail

E-mail is considered network activity. Thus, it is subject to all policies regarding acceptable/unacceptable uses of the Internet and the user should not consider e-mail to be either private or secure. Users should be aware that E-mail which has been sent on an informal basis will be subject to the same levels of screening as those which are perceived to be official. Messages sent and received via the Internet are regarded as having the same legal status as a corporate letter.

19. Confidentiality

Any material that is viewed as sensitive, personal, highly confidential or valuable to the service should not be e-mailed externally. It should be remembered that the Internet does not guarantee delivery or confidentiality.

It should be noted that there are systems in place that can monitor, review and record all e-mail usage, and these will be used. Analysis of this information may be issued to managers if thought appropriate. No user should have any expectation of privacy as to his or her e-mail.

20. Related Policies & Documents

- Employee Remote Access Policy
- Employee Remote Access Procedure
- Third Party Remote Access Policy
- Third Party Remote Access Procedure

21. Equality Impact Assessment

This procedure was impact assessed on 01 APR 09.

22. Review

This procedure will be reviewed on a 3 yearly basis.

Next Review: 2012