HUMBERSIDE FIRE AND RESCUE SERVICE

SERVICE DELIVERY SUPPORT

INTERNET, E-MAIL & INSTANT MESSAGING POLICY

Owner	**Director of Service Delivery Support**
Responsible Person	**Head of ICT**
Date Written	**February 2010**
Date of last review	**January 2021**
Date of next review	**August 2021**

CONTENTS

1. INTRODUCTION

This Policy applies to the use of any ICT facilities, including hardware, software and networks, provided by the Service for the purposes of sending or receiving e-mail messages and attachments, communicating internally through instant messaging and applies to the use of the internet for retrieval of information. The guidance is applicable to all employees, Elected Members and other authorised users of the Service's internet, e-mail and instant messaging and facilities.

Guidance provided here extends to mobile devices that provide internet access, remote (or push) e-mail and instant messaging capability, including smart phones, tablets etc.

2. POLICY STATEMENT

The Service encourages the effective use of the internet, e-mail and instant messaging as tools to add value to the work of the Service and assist in meeting organisational objectives.

Users of these facilities are responsible for making sure their activities:

- support the Service's work and values;
- maintain the confidentiality, integrity and availability of the Service's information and computer systems;
- are lawful and do not damage the Service's reputation.

3. EQUALITY AND INCLUSION

HFRS has a legal responsibility under the Equality Act 2010, and a commitment, to ensure it does not discriminate either directly or indirectly in any of its functions and services nor in its treatment of staff, in relation to race, sex, disability, sexual orientation, age, pregnancy and maternity, religion and belief, gender reassignment or marriage and civil partnership. It also has a duty to make reasonable adjustments for disabled applicants, employees and service users.

4. AIM AND OBJECTIVES

The purpose of this Policy is to minimise the risks to the security and integrity of the Service's ICT infrastructure by:

- providing clear guidance to users on actions and behavior that is acceptable and that which is not;
- informing users of the manual and technical solutions which are deployed to assist in protecting the ICT environment; and
- informing users about the requirements of relevant legislation.

5. INTERNET, E-MAIL AND INSTANT MESSAGING USE

Users of internet, e-mail and instant messaging shall have regard to the following conditions:

Personal Use

Personal use is defined as any activity:

- solely related to an individual acting in their private capacity (regardless of whether any direct or indirect personal benefit is gained);
- is not directly linked to the development, improvement or delivery of organisational objectives or Service's work; and,
- is not part of the user's professional development.

Personal use of the internet, e-mail and instant messaging is permitted only during designated rest periods, and only where the user has agreed that their usage can be monitored by the Service. Personal use during those periods is still subject to the usage arrangements described below. Should bandwidth or other issues be adversely affected by personal use, then this permission may be withdrawn by the Service Support Directorate without consultation, although users will be informed if this is the case.

Official Use

Official use is defined as activity relating to:

- supporting organisational objectives;
- the user's current or future potential role;
- professional or work-related personal development; or,
- maintaining awareness of news and current affairs, particularly relating to role specific subjects or wider fire and rescue service issues.

Users are required to be aware that internet browsing, e-mail and instant messaging have the potential to cause significant damage to computer systems and other aspects of the organisation, including reputation.

Users shall observe the following guidance:

General Guidance

Users shall:

- keep their user credentials secure and in accordance with the Information Security Policy;
- comply with license terms and conditions when copying, downloading or sending material covered by copyright law;

- immediately contact the ICT Service Desk if they suspect any webpage accessed, email or instant message contains malicious code (e.g. virus, key logger) or before downloading software from the internet or from an e-mail; and
- have due regard to the Data Protection Act 2018 when placing personal data in newsgroups, on web sites, in messages or as e-mail attachments and be aware that such communications will be subject to disclosure under the Freedom of Information Act 2000 (subject to any statutory exemption).

Users shall not:

- compromise the security of their user credentials by leaving systems in a condition that would enable other employees to access these facilities through that account;
- commit the Service to purchasing or acquiring goods or services using the internet or e-mail without obtaining prior approval and following relevant Finance Section guidance;
- use anonymous mailing services to conceal their identity, falsify e-mails to make them appear to originate from someone else, or provide false information to any internet service which requests name, e-mail address or other details;
- carry out political lobbying or private business;
- knowingly doing anything which is illegal under English law; or
- intentionally accessing or transmitting computer viruses and similar software (or information about, or software designed for, breaching security controls or creating computer viruses).

E-mail and Instant Messaging Guidance

E-mail and instant messaging is never completely confidential or secure. Messages may appear to be temporary by nature, but they can be widely distributed and easily retrieved. E-mail communications, either internally or on the internet, are not guaranteed to be private or to arrive at their destination either within a certain timeframe, or at all. For the purposes of this guidance, e-mail relates to both internal and external messages.

Users shall:

- always consider whether e-mail or instant messaging is the best method of communication, taking account of latency in delivery, need to present an appropriate professional image and potential for others to access such communication;
- comply with the Information Classification Policy when forwarding information by e-mail, posting details on internet sites or sending instant messages;
- have an automatic disclaimer and include contact details of the sender (e.g. telephone number, e-mail address etc.) A disclaimer is automatically added to all mail to external recipients;

- subject e-mail, instant messages activity to the same standards of quality control as paper documents, this includes recognition that e-mail bears the same legal standing as other written advice;
- have due regard to the Data Retention Schedule for the timescales that e-mail messages need to be kept;
- seek line manager approval before subscribing to news or alert services, professional interest groups or similar;
- manage their e-mail account efficiently, including using the out of office assistant, archiving messages, etc; and
- inform Corporate Assurance (dataprotection@humbersidfire.gov.uk) immediately they become aware that any e-mail they have sent or, have received, may have been mis-directed or received by the wrong recipient.

User shall not:

- carbon copy (cc or bcc) higher level managers into their e-mail messages as an attempt to assume tacit approval of content;
- create auto-forwarding rules to copy all inbound e-mail to an external e-mail account without permission from the ICT Section and without regard to the Information Classification Policy;
- forward e-mail chain letters or participate in pyramid or similar schemes;
- abuse others, even in response to abuse directed at them;
- send unsolicited, irrelevant or inappropriate e-mail;
- use e-mail or instant messaging to sexually harass, bully, threaten or defame anyone; or
- forward material of a personal nature to others without the permission of the originator.

Users should be aware that in certain circumstances, monitoring or re-directing of emails is permissible where there is a clear organisational need. A written request must be made by the Head of Function to the appropriate Director and, provided written approval is given by the Director, IT will carry out the necessary arrangements. Access will be restricted to a named individual or individuals at a suitable level within the organisation and a decision reached between the Head of Function and Director as to whether emails are monitored or re-directed. The affected member of staff will be notified by the Head of Function or Director prior to the arrangement being made, and an appropriate “Out of Office” reply will be placed on the email account. Any such arrangement must be terminated as soon as the need ceases, but in any case, no later than the return to work of the absentee.

Internet Guidance

Users shall:

- immediately report to the ICT Service Desk and their Line Manager details of any web sites accidentally accessed that contained inappropriate material, as

outlined in 'Inappropriate Use' below, so that this can be taken into account during any monitoring;
- report instances of suspected misuse to a line manager for further investigation;
- be aware that information from the internet may not be accurate or correct and verify that information whenever needed;
- undertake internet browsing for specific purposes, keeping on-line time to a minimum; and
- log off immediately after use.

Users shall not:

- use the internet to watch or capture live television images;
- unnecessarily stream video, audio or similar content from the internet which requires high bandwidth;
- download browser plug-ins or similar applications without prior authorisation from the ICT Section;
- access external e-mail systems (such as hotmail, gmail, etc.);
- do anything which would adversely affect the ability of others to access internet resources;
- break through, or attempt to break through, security controls, whether on the Service's equipment or on any other computer system;
- access internet traffic (such as e-mail) not intended for him/her, even if not protected by security controls; or
- carry out any activities which could cause congestion or disruption to networks or systems. This includes using e-mail addresses for creating online accounts to purchase goods or services of a personal nature or to receive mailing of offers, etc.

Inappropriate Use

Users shall not access or attempt to access, display, download, copy, forward or circulate any information of the following nature:

- pornography (including child pornography) or sexually orientated images
- gambling
- gaming (playing computer games)
- promoting or containing unlawful discrimination of any kind
- promoting or containing racial or religious hatred
- involving threats including promotion of violence
- promoting illegal acts

- any other information which may reasonably be considered as offensive, inappropriate or disrespectful to others, or damage the reputation of the Service, and
- unauthorised copyrighted material, including music, video and pictures.

The Service will report all known incidents, in which users do, or appear to have, intentionally accessed websites, newsgroups, online groups or distributed e-mail that contain the following type of material, to the police for investigation.

- Images of child pornography or child abuse (i.e. images where children are or appear to be under the age of 16 and are involved in sexual activities or posed to be sexually provocative).
- Adult material/pornography that potentially breaches the Obscene Publications Acts (1959 & 1964).
- Criminally racist material.

Viruses

Deliberate introduction of any damaging virus is a crime under the Computer Misuse Act 1990. Most of the organisation's computer equipment has virus checking software installed and virus checking facilities are widely available.

It is the responsibility of individual users to ensure that all computer files are virus-free. Internet e-mail virus checking will be carried out as part of the facilities from an external supplier, but users still need to remain vigilant.

If material is inadvertently accessed which is believed to contain a computer virus, a user shall immediately break the connection, stop using the computer, and contact the ICT Section. Advice or information on virus checking can be obtained from the ICT Section.

6. MONITORING

Managers may inspect any e-mail correspondence or instant message within their department to see if users are complying with the policy. Similarly, appropriate members of the ICT Section may inspect any e-mail correspondence or instant messages to ensure compliance with this policy and to maintain integrity of the systems. Any potential misuse identified from monitoring will be reported to the ICT Section in the first instance. Serious breaches of this policy will amount to gross misconduct and may result in action under the Disciplinary Policy.

The Service reserves the right to:

- monitor users' access to or use of, any computer system or communications service, to see whether they are complying with the policy;
- withdraw users' access to any computer system or communications service, including internet, e-mail and instant messaging facilities;

- prohibit access to certain specific newsgroups, web pages or other computer resources;
- prevent the receipt of e-mail messages which are out of context with the work of the Service or contain viruses or are spam*; and
- remove or substitute the hardware or software used to access the internet and e-mail at any time and for any reason.

***** Spam is junk e-mail, often unsolicited. Filtering is in place to intercept spam messages before they reach user accounts. Users who continue to receive this sort of e-mail should contact the ICT Section to see if the filtering can be refined.

The right to monitor activity does not automatically extend to e-mail or instant messages between an employee and recognised representative bodies, except where inappropriate use of these facilities is identified. Random sifts to ensure compliance with this policy shall exclude such communications.

If it is found that the internet access, e-mail or instant messaging is being used in contravention of this guidance, the user may be subject to action under the Disciplinary Policy. The Service may respond to contraventions by any combination of:

- informal warning.
- denial of internet access for a period of time, or permanently.
- withdrawal of facilities for a period of time, or permanently.
- action through the Disciplinary Policy.
- supply information to the police for investigation and possible criminal proceedings.

7. COPYRIGHT OF ALL E-MAIL, INSTANT MESSAGES AND INTERNET POSTINGS

The Service shall own in perpetuity, all intellectual property (rights, title and interests) and images (including but not limited to all designs and copyright) which are created, in whole or in part, whether directly or indirectly, by any employee during the term of their employment.

The employee shall not in any way, deal or interfere with any intellectual property rights of the Service. No intellectual property will vest in the employee and the employee shall not make any claim as to any right, title or interest accordingly.

Where the employee seeks to use any intellectual property rights of the Service for a purpose other than their employment, then the Service may consider such a request in writing by an authorised officer. Such a grant will be by way of a licence and no right, interest or title will transfer.

If anyone requires any further guidance / information relating to this document, please contact ICT.