



HUMBERSIDE FIRE AND RESCUE SERVICE

Service Improvement

Internet, Email and Instant Messaging Policy

Owner	Executive Director of Corporate Services
Responsible Person	Head of Digital Solutions
Date Written	February 2010
Date of last review	May 2024
Date of next review	May 2025
EIA Completed	August 2021



What we must do well



How we support our communities



We value and support the people we employ



We efficiently manage the Service

CONTENTS

1. [Introduction](#)
 - [Core Code of Ethics](#)
 - [National Guidance](#)
2. [Equality, Diversity and Inclusion](#)
3. [Aim and Objectives](#)
4. [Associated Documents](#)
 - [Equality Impact Assessment](#)
 - [Legal References](#)
 - [National Guidance](#)
5. [Policy Statement](#)
6. [Internet, Email, and Instant Messaging Use](#)
 - [Personal Use](#)
 - [Official Use](#)
 - [General Guidance](#)
 - [Email and Instant Messaging Guidance](#)
 - [Internet Guidance](#)
 - [Inappropriate Use](#)
 - [Viruses](#)
7. [Monitoring](#)
8. [Copyright of all Email, Instant Messages, and Internet Postings](#)
9. [Appendix A: Microsoft Teams Management Protocol](#)

1. INTRODUCTION

This Policy applies to the use of any Digital facilities, including hardware, software, and networks, provided by the Service for the purposes of sending or receiving email 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, email and instant messaging and network facilities.

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

Core Code of Ethics

Humberside Fire & Rescue Service (HFRS) has adopted the Core Code of Ethics for Fire and Rescue Services. The Service is committed to the ethical principles of the Code and strives to apply them in all we do; therefore, those principles are reflected in this Policy.

National Guidance

Any National Guidance which has been adopted by HFRS, will be reflected in this Policy.

2. EQUALITY, DIVERSITY 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 or 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.

3. AIM AND OBJECTIVES

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

- Providing clear guidance to users on actions and behaviour that is acceptable and that which is not.
- Informing users of the manual and technical solutions which are deployed to assist in protecting the Digital Infrastructure environment.
- Informing users about the requirements of relevant legislation.

4. ASSOCIATED DOCUMENTS

- [Equality Impact Assessment](#)

- [Data Protection Impact Assessment Template](#)
- Legal References
 - [Data Protection Act 2018](#)
 - [Freedom of Information Act 2000](#)
 - [Computer Misuse Act 1990](#)
- National Guidance Reference
There is no specific National Guidance relevant to this policy.
- [Data Protection Policy](#)

5. POLICY STATEMENT

The Service encourages the effective use of the internet, email, 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.

6. INTERNET, EMAIL, AND INSTANT MESSAGING USE

Users of internet, email 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).
- Not directly linked to the development, improvement or delivery of organisational objectives or Service's work.
- Not part of the user's professional development.

Personal use of the internet, email 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 Improvement 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.
- 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, email 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 Digital Solutions Service Desk if they suspect any webpage, email, or instant message accessed contains malicious code (e.g., virus, key logger) or before downloading software from the internet, or from an email.
- Have due regard to the [Data Protection Act 2018](#) when placing personal data in newsgroups, on web sites, in messages or as email 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 or by divulging their user credentials to anyone else.
- Commit the Service to purchasing or acquiring goods or services using the internet or email without obtaining prior approval and following relevant Finance Section guidance.
- Use anonymous mailing services to conceal their identity, falsify emails to make them appear to originate from someone else, or provide false information to any internet service which requests name, email address or other details.
- Forward any information to a personal email address.

- Carry out political lobbying or personal business.
- Knowingly doing anything which is illegal under English law.
- Intentionally access or transmit computer viruses and similar software (or information about, or software designed for, breaching security controls or creating computer viruses).

Email and Instant Messaging Guidance

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

Users shall:

- Ensure they have tested that external email addresses are legitimate and correct before deciding to send any communication.
- Bcc should be used where recipients should not be aware of who else has also been emailed, which may include internal, external, or personal email addresses.
- Where Bcc is used then an instruction at the bottom of the email advising not to reply using the “reply all” function should always be included.
- On the realisation of an incorrect email being sent, then the Outlook recall facility can be used, however this is limited, and not always reliable as it is dependent on the email client being used by the recipient.
- In all cases of an incorrect email being sent then the recipient should be contacted immediately and be requested to delete the email and any attachments included.
- Any potential breach of GDPR due to incorrect emails being sent should be reported to databreach@humbersidfire.gov.uk immediately.
- Always consider whether email 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 email, posting details on internet sites, or sending instant messages.
- Have an automatic disclaimer and include contact details of the sender (e.g., telephone number, email address etc.). A disclaimer is automatically added to all mail to external recipients.
- Subject emails and instant messages activity, to the same standards of quality control as paper documents. This includes recognition that email bears the same legal standing as other written advice.

- Have due regard to the Automatic Retention Schedule ([see Appendix A](#)) for the timescales that email, chat, Teams chat, and channel messages/documents need to be kept, these being:
 - Email - An automatic retention schedule deletes emails monthly that are more than 1 year old.
 - MS Teams -
 - Individual chat automatic retention schedule deletes any chat over 30 days old.
 - Teams chat - automatic retention schedule deletes any chat older than 365 days (1 year).
 - Files in Teams & channels - automatic retention schedule deletes documents older than 365 days (1 year) from the date last modified.
- Seek line manager approval before subscribing to news or alert services, professional interest groups or similar.
- Manage their email account efficiently, including using the out of office assistant, archiving messages, etc.
- Inform databreach@humbersidefire.gov.uk immediately they become aware that any email 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 email messages as an attempt to assume tacit approval of content.
- Create auto-forwarding rules to copy all inbound email to an external email account without permission from the Digital Solutions Section, and without regard to the Information Classification Policy.
- Forward email chain letters or participate in pyramid or similar schemes.
- Forward on any information to a personal email address.
- Abuse others, even in response to abuse directed at them.
- Send unsolicited, irrelevant, or inappropriate email.
- Use email or instant messaging to sexually harass, bully, threaten, or defame anyone.
- Forward material of a personal nature to others without the permission of the originator.

Internet Guidance

Users shall:

- Immediately report to the Digital Solutions 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 considered 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.
- 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 Digital Solutions Section.
- Access external email 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 email) not intended for him/her, even if not protected by security controls.
- Carry out any activities which could cause congestion or disruption to networks or systems. This includes using email 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 be considered as offensive, inappropriate, or disrespectful to others, or damage the reputation of the Service.
- 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 email 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 email 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 Digital Solutions Service Desk immediately. Advice or information on virus checking can be obtained from the Digital Solutions Section.

7. MONITORING

Managers may inspect any email correspondence or instant message within their department to see if users are complying with the policy. Similarly, appropriate members of the Digital Solutions Section may inspect any email 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 Digital Solutions 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, email, and instant messaging facilities.
- Prohibit access to certain specific newsgroups, web pages or other computer resources.
- Prevent the receipt of email messages which are out of context with the work of the Service or contain viruses or are [spam](#)*.

- Remove or substitute the hardware or software used to access the internet and email at any time and for any reason.

* Spam is junk email, often unsolicited. Filtering is in place to intercept spam messages before they reach user accounts. Users who continue to receive this type of email should contact the Digital Solutions to see if the filtering can be refined.

The right to monitor activity does not automatically extend to email 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, email, 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.

Personal use

Although the email system and our instant messaging tools are primarily for business use, we understand that you may on occasion need to use these to send or receive personal emails. When sending personal emails or instant messages, you should show the same care and attention and comply with the same obligations as when sending work-related emails.

Access to the Service's computer systems is provided for Service-related business purposes. To protect the Service's legitimate business interests, we may monitor and/or record your email and instant messaging usage if:

- You are absent for any reason and communications must be checked to ensure business continuity can be maintained ([see Service Need below](#)).
- We suspect that you have been viewing or sending offensive, obscene, defamatory, discriminatory, intimidating, malicious, insulting or otherwise inappropriate or illegal material.
- We suspect excessive personal use.
- We suspect that you are sending or receiving emails that are detrimental to the service and/or in breach of data protection legislation.
- We have grounds for suspecting criminal activity.
- It is necessary to investigate a grievance or disciplinary matter.

When monitoring emails, unless there are exceptional circumstances, we will restrict ourselves to looking at the address and subject heading.

You should mark any personal emails as "private" or "personal" in the subject line and encourage those who send them to do the same. Where possible, we will avoid opening emails clearly marked as private or personal.

Service Need

Users should be aware that in certain circumstances, monitoring or re-directing of emails is permissible where there is a clear organisational need. 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.

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. 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.

A written request must be made by the Head of Function to the appropriate Area Manager (AM) and, provided written approval is given by the AM, Digital Services will carry out the necessary arrangements. Access will be restricted to a named individual or individuals at a suitable level within the organisation.

Data protection

If we decide to monitor your email, instant messaging and internet usage, it will be in response to a specific need and for the purposes of our legitimate interests, namely, to ensure that this policy is being complied with.

Monitoring will be carried out in compliance with data protection laws and will be conducted in accordance with a data protection impact assessment (DPIA) that we have carried out to ensure that any monitoring we carry out is necessary and proportionate.

To contact the Information Governance Officer email: dataprotection@humbersidefire.gov.uk. Monitoring will normally be conducted by the Head of Digital Services, or in their absence, the Digital Assurance Data & Applications Manager.

The technology that we use to monitor your email, instant messaging and internet usage includes O365 Security and Compliance Monitoring Centre and CrowdStrike.

Any information obtained through monitoring may be shared internally, including with the Strategic Leadership Team, members of the HR team, your line manager, managers in the Service area in which you work and IT staff, if access to the data is necessary for performance of their roles. However, information would normally be shared in this way only if we have reasonable grounds to believe that there has been a breach of the rules set out in this policy.

The information gathered through monitoring will be retained only long enough for any breach of this policy to be identified and for any investigation to be conducted. Data is normally securely destroyed in line with our Retention Schedule.

Information obtained through monitoring will not be disclosed to third parties (unless we are under a duty to report matters to a regulatory authority or to a law enforcement agency).

You have a number of rights in relation to your data, including the right to make a subject access request and the right to have data rectified or erased in some circumstances. You can find further details of these rights and how to exercise them in our [Data Protection Policy](#). If you believe that the Service has not complied with your data protection rights, you can complain to the [Information Commissioner](#).

8. COPYRIGHT OF ALL EMAIL, 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 Digital Solutions.

APPENDIX A: MICROSOFT TEAMS RECORDS MANAGEMENT PROTOCOL

1. Introduction

This protocol sets out how information is managed within Microsoft Teams. Like all information held by the Service, information in Microsoft Teams should have a lifecycle.

Microsoft Teams is a collaboration tool, anything shared in Microsoft Teams should be transient, it **must not** be used as the final resting place of any file.



2. Teams Owner(s) and Permissions

A team **must have more than one Owner** to ensure business continuity, for example if one Owner leaves the Service or is on a period of absence.

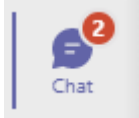
The Owner(s) of Teams are responsible for the management of that Team. This includes:



- Ensuring membership remains correct and that Teams and its channels are used appropriately by all members.
- Assigning members of Teams with the correct permissions.
- Admit any external members (known as guests in Teams);
- Remove members when their inclusion is no longer needed.
- Managing files associated with Teams and channels.
- Delete Teams, channels, and files when they are no longer needed.

3. Use of Microsoft Teams

Microsoft Teams is a collaborative tool where colleagues can come together to share ideas and work on documents/files simultaneously. Each element of Microsoft Teams is intended to be used for a specific purpose by the Service. **Microsoft Teams should only be used as a collaboration tool and not for long-term storage or relied upon for evidence of decision making on a long-term basis.**

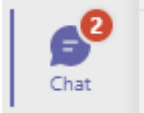



The following table outlines how different elements of Microsoft Teams should be used:

MS Teams Element	Use
 <p>Chat</p>	<p>Chat should be used as the name suggests, for chat between staff in the same way discussions take place in the office. Chat should ideally take place on a 1-2-1 basis but can involve multiple people. Chat messages are often more informal than Teams Chat messages.</p> <p><i>All messages are still auditable and may be subject to release under disclosure regimes such as Freedom of Information and Data Protection legislation.</i></p> <p>Files and documents should not be routinely shared within Chat.</p> <p>Any discussions which are intended to be kept for longer than 30 days should take place in a Team or channel.</p>

MS Teams Element	Use
 Teams and Channels	<p>Teams and channels should be used to have discussions about Service business. They can also be used to share documents and arrange meetings.</p> <p>Channels should be set up to cover themes or areas of work which make sense for the people/team wanting to use them.</p> <p><i>Teams may include external people from other organisations and so should only discuss or share documents that the external person is allowed to see.</i></p>
 Files in teams and channels	<p>Files shared in Teams and channels are saved in SharePoint. This is because when a Team is created a new SharePoint site is created in the background.</p>

4. Destruction and Retention

Microsoft Teams is a transient collaborative tool and as such chats and files will be automatically deleted in line with the following destruction and retention policies:

MS Teams Element	Retention Period	
1-2-1 chat, group chat and meetings	 Chat (including meetings and group chat)	<p>30 days of chat history will be retained.</p>
	 Documents in Chat (including meetings)	<p>NB files shared in chat, group chat or meetings are saved in the 'Microsoft Teams Chat Files' folder of the person's OneDrive who shared them. These files are not deleted from an individual's OneDrive when a chat or meeting is deleted. It is an individual's responsibility to manage their own OneDrive Teams Chat folder in accordance with other retention schedules.</p>
Teams and channels	 Teams Chat	<p>365 days (1 year) of team history will be retained.</p> <p>The retention period outlined above is the default period, the Owner(s) of the Team can still delete the Team at any time.</p>
	 Files in teams and channels	<p>Files shared in Teams and channels are saved in SharePoint. This is because when a Team is created a new SharePoint site is created in the background.</p> <p>Teams' files and documents will be retained for a maximum of 365 days (1 year) from the date last modified.</p> <p>If the Owner deletes a Team, the associated files are deleted. However, if the Owner deletes a regular channel the associated documents are not deleted, they remain in SharePoint. If the</p>

**Digital Solutions
Internet, Email, and Instant Messaging Policy**

MS Teams Element		Retention Period
		<p>Owner deletes a private channel the associated documents are deleted.</p> <p>Files that need to be shared for longer periods should be saved in line with existing records management practices.</p> <p>This is to prevent important information being deleted if the channel is deleted when files or documents are shared elsewhere.</p> <p>Owners must delete documents before closing a channel or documents should be deleted once they have been finalised with to avoid duplication.</p>