

MERSEYSIDE FIRE AND RESCUE AUTHORITY			
MEETING OF THE:	POLICY AND RESOURCES COMMITTEE		
DATE:	1ST APRIL 2014	REPORT NO:	CFO/031/14
PRESENTING OFFICER	KIERAN TIMMINS DEPUTY DEPUTY CHIEF EXECUTIVE		
RESPONSIBLE OFFICER:	KIERAN TIMMINS HEAD OF TECHNOLOGY	REPORT AUTHOR:	ED FRANKLIN
OFFICERS CONSULTED:	RIA GROVES – TRAINEE SOLICITOR PETER RUSHTON – DIRECTOR OF CORPORATE COMMUNICATIONS NICK MERNOCK – DIRECTOR OF PEOPLE & ORGANISATIONAL DEVELOPMENT DEB APPLETON – DIRECTOR OF STRATEGY & PERFORMANCE		
TITLE OF REPORT:	ACCESS TO SOCIAL MEDIA		

APPENDICES:	APPENDIX A	SI0699 – USING SOCIAL MEDIA
--------------------	-------------------	------------------------------------

Purpose of Report

1. To request authority approval for ICT to open up access to Social Media Sites on the corporate network for all Merseyside Fire & Rescue Service (MFRS) staff.

Recommendation

2. That Members;
 - a) Note recent upgrade of Websense, the corporate Web Filtering and Email filtering solution
 - b) Approve the access to Social Media on the Corporate ICT Network for all staff
 - c) Note the mitigation measures in place to avoid abuse or misuse

Out Comes of Using Social Media

- Promote Merseyside Fire & Rescue Authority (MF&RA) Corporate Communications Strategy
- Promote and deliver MF&RA work and the positive outcomes in and to our community

- Using social media in the work place not just for staff to stay in touch with family and friends but to be more productive and effective in their work
- Connecting and maintaining relationships with other fire and rescue services and partners

Introduction and Background

3. Social media is the name commonly given to Interactive Communication Technology websites; primarily those which enable users to interact and communicate by sharing content such as opinion, media (video, images and audio), knowledge and interests.
4. Typically, social media contributes to the building of 'networks' or online communities while encouraging participation and engagement. The term encompasses many variations of online media. Examples include blogs, micro-blogs (Twitter), podcasts, 'wikis' (such as Wikipedia), message boards, social book marking websites (Reddit), social networking websites (Facebook, MySpace) and media content sharing websites (such as Flickr, YouTube).
5. Corporate Communications have access to Facebook and Twitter and they are responsible for the Merseyside Fire & Rescue Service (MFRS) presence in the Social Media Community. There are pockets of social media activity by various departments such as Youth Engagement.
6. The Authority has in place an ICT Acceptable Usage Policy (ICTPOL03) which covers a number of Service Instructions (SI) including the SI relevant to this report, SI0699 Using Social Media.
7. This SI will ensure that all MFRS personnel recognise the importance of new and emerging media platforms for communicating and consulting with the public, whilst engaging in these new methods of communication in a responsible, coordinated and consistent manner.
8. The corporate Web Filtering and Email filtering solution for staff accessing the internet on their MF&RA computer is the Websense system.
9. Websense has in built management reporting of user activity and statistics which are presented to Level 6 Budget Managers on a monthly basis via the ICT Infrastructure Report.
10. In the past Websense only offered complete granular control of all corporate access to the internet and email. This control has now been extended to Social Media sites in the latest available upgrade.
11. The upgrade version of Websense has been successfully completed

Actions to be taken

12. If open access is approved continue with this action list.

13. Progress the Service Instruction 'SI0699 Using Social Media' through consultation process estimated at 21 days.
14. When in place send a communication out to all staff including highlighting the Social Media SI.
15. Action a simple change to the Websense configuration opening up Social Media to all staff on the Corporate Network
16. ICT will amend the ICT Infrastructure Usage report to include user activity & statistics in the area of social media. This is made available to Level 6 Budget Managers.
17. MF&RS staff must comply with SI0699 Using Social Media Policy and will continue to work closely with and seek permission from Corporate Communications to ensure any future Social Media initiatives are aligned to the Corporate Strategy.

Equality and Diversity Implications

18. This initiative has a positive impact for all Equality Groups with no perceived negative concerns. Consultation with the Equality and Diversity Consultation Manager has ascertained there is no requirement to produce a full Equality Impact Assessment (EIA).

Staff Implications

19. Advantages of allowing the use of social media at work:
 - Improved efficiency and productivity.
 - Increased Loyalty.
 - Improved Employee Satisfaction.
 - Attracting the right kind of talent. Generation X and Y individuals.
 - Workplace Harmony
 - Managers can manage staff usage supported by, amongst other controls, the Infrastructure Usage Report
20. Dis-advantages of allowing the use of social media at work:
 - Employees can waste time
 - Detracts from their normal jobs
 - Companies can be portrayed in a bad light by a negative employee
 - Decreases productivity

Legal Implications

21. The use of social media does not come without legal implications for any business or individual.

22. The biggest risk to an employer is the improper use of public electronic communications networks by employees. In particular the risk the Authority may be exposed to through use of social media is breaches of the Data Protection Act and Defamation actions committed by employees.
23. There are also serious risks to be considered in respect of the Regulation of Investigatory Powers Act 2000 (RIPA) whereby surveillance may deliberately or accidentally take place. For example the Facebook page or Twitter account of a particular individual could be being monitored for purposes of preventing or detecting crime. This would be described as covert surveillance in many circumstances and although it may be inadvertent, it must be authorised via RIPA procedures before it can take place to ensure that such surveillance is proportionate and does not unnecessarily breach Human Rights.
24. Although surveillance of employees for legitimate purposes does not technically fall under RIPA, it must nevertheless be authorised by an alternative route to ensure that Human Rights are properly considered and protected and that there is accountability and an audit trail of decisions.
25. The Clerk to the Authority is able to advise any employee of the correct approach to authorisation or both employees and non-employees
26. Additionally criminal activities that may be carried out by employees whilst at work such as online harassment, public disorder offences (threats made against another individual on a website, forum or social network that will be seen by the intended target) and incitement of racial hatred online present a real reputational risk to the Authority or may even hold the Authority to be vicariously liable if such activities have been carried out during their employment and as a representative of the Authority.
27. However as these risks to the Authority are already present through any employees use of social media outside of work hours implementing social media access within Authority premises will not greatly increase the risks referred to above particularly if the social media policy addresses the way in which sites are used (for example social media is only accessed in employees own time such as their lunch break) and there are rules of engagement with social media users, monitoring of channels and employees communication (for example uploading of videos of confidential data at work).

Financial Implications & Value for Money

28. This initiative is possible due to the software upgrade of Websense the cost of which was covered within the ICT current budget.

Risk Management, Health & Safety, and Environmental Implications

29. The main risk of using social media as an organisation would be the potential damage to reputation due to misuse.

30. There is also the risk of damage to an individual's personal and/or professional reputation.
31. Social Networks are having a greater risk of exposing the organisation to virus and malware threats. This is because users place too much trust in people within their social network, even though they may not know the people in real life. Consequently users are more likely to click on a link within Twitter, Facebook or LinkedIn than in an email, where most people today are a little more circumspect.
32. Tools such as Websense, however, are becoming more sophisticated in protecting the Corporate ICT Infrastructure from such risks.

Contribution to Our Mission: *Safer Stronger Communities – Safe Effective Firefighters*

33. Use of Social media will make a positive difference to the community of Merseyside and enable our people to be the best they can be.

BACKGROUND PAPERS

20/10/2013 Re-issue of previous SMG Report with newly attached Service Instruction

GLOSSARY OF TERMS

EIA	Equality Impact Assessment
ICT	Information and Communication Technology
MFRA	Merseyside Fire and Rescue Authority
MFRS	Merseyside Fire and Rescue Service is the service provided by MFRA.
POD	People and Organisational Development
SI	Service Instruction