Finance and Resources Committee 17 March 2011

# New employee policy: Social Media Policy

## Executive summary and recommendations

### Background

The attached draft Social Media Policy is an entirely new employee policy, designed to clarify the HPC's expectations of employees in the appropriate use of social media tools. It has been developed to support the implementation of the HPC's Social Media Strategy, which aims to promote the HPC's work by engaging with users of a wide range of social media tools.

The policy has been drafted with input from the HR, IT and Communications Departments, and has been sent to all employees for comment.

The draft Social Media Policy is intended to complement the HPC's Information Technology policy, a copy of which has been provided for information.

### Decision

The Committee is requested to approve the new Social Media Policy.

### Resource implications

None

### Financial implications

None

### Appendices

Appendix I – draft Social Media Policy
Appendix II – Information Technology Policy (Employee Handbook section 5h)

### Date of paper

7 March 2011

**Appendix I**

**Draft Social Media Policy**

## 1. Purpose

1.1 This policy clarifies expectations of HPC employees when using social media for both business and personal use. It addresses the posting or submitting of comments or content, as well as access to view web published content on social media sites.

It complements and should be read in conjunction with the IT policy, which sets out the requirements of employees when using all of the HPC's electronic and IT systems and equipment.

This policy has been developed to support the implementation of the HPC Social Media strategy, which aims to promote the HPC's work by engaging with users of social media.

## 2. Social media

2.1 Social Media are web based technologies that enable social interaction. They include but are not limited to:

- Social networking sites (Facebook, MySpace, Foursquare)
- Video and photo sharing websites (Flickr, YouTube)
- Micro-blogging sites (Twitter)
- Blogs
- Forums and discussion boards (e.g., local discussion boards, Whirlpool, Yahoo! Groups or Google Groups)
- Online encyclopedias (e.g., Wikipedia, Sidewiki)

2.2 This policy covers the following types of use, collectively referred to as 'Social Media Tools':

a. Formal HPC presence and
b. Informal, non-contractual HPC presence, whether they are HPC-branded or not

and is applicable to:

a. Any social media sites when publishing content; and also
b. general access to view content to the following:

- Social networking sites (Facebook, MySpace, Foursquare, LinkedIn)
- Video and photo sharing websites (Flickr, YouTube)
- Micro-blogging sites (Twitter)

2.3 'Business use' is defined as access to, or publishing of content on any social media tool which results in a clear business benefit as set out in paragraph 3.1 below.

2.4 'Personal use' is defined as access to, or publishing of content on any social media tool for which employees are pursuing their own interests and for which there is no clearly defined business benefit.

## 3. Policy for business use of social media

3.1 The HPC will grant access to social media tools to specific employees in support of their role, where there is a clear business benefit provided and where they have written approval from the relevant Director. Authorisation to use social media tools is granted on the basis of business use only and individual usage will be monitored.

3.2 The Communications department is responsible for deciding which social media tools the HPC should use for business purposes, and for monitoring and uploading HPC-related content.

3.3 Social media content must not bring the HPC into disrepute and only publicly available information may be disclosed. The HPC requires employees using social media tools on behalf of the HPC to:

- Access the HPC/ professional aspect of the relevant site, rather than their personal profile pages
- Identify themselves as working for the HPC, either through their profile or through their name
- Ensure that they do not conduct themselves in a way that is detrimental to the reputation of the HPC
- Take care not to allow their interaction on these websites to damage working relationships between employees, registrants, partners, or any other HPC stakeholders
- Ensure any information published on these websites has been through the necessary checks to promote accuracy
- Ensure that no information is made available that could provide a person with unauthorised access to commercially sensitive and/or any confidential information
- Ensure that their use of social media tools complies with all of the provisions of the HPC IT policy

3.4 Fuller practical guidance on using social media for business purposes is available online or from the Communications Department. Employees must familiarise themselves with this guidance before representing the HPC via social media.

## 4. Policy for personal use of social media

4.1 The HPC does not allow access to social media tools for personal use from its IT systems. Access to some sites is blocked completely. However, the HPC recognises that many employees participate in social networking outside of work on websites such as Facebook, Twitter and MySpace. Employees are fully entitled to carry out these activities provided that they follow the advice set out in the following paragraphs.

4.2 Be careful of how you represent yourself on social networks as the lines which differentiate between what is public or private and what is personal or professional are becoming increasingly blurred.

4.3 Be aware that social networking websites can act as public forums, and that 'confidential' areas of sites may not have reliable security controls.

4.4 If you identify yourself as working for the HPC in social networks you should ensure that content associated with you as an identifiable HPC employee is consistent with your role in the organisation and does not compromise the HPC's reputation.

4.5 Remember that you may be connected or visible to HPC colleagues, members, registrants and partners. Unless you go to extraordinary lengths to keep your online content private, be sure to manage what information you are sharing and with whom.

4.6 Do not make available information that could provide a person with unauthorised access to commercially sensitive and/or any confidential information.

4.7 Do not comment on work related issues or on the HPC's business.

4.8 HPC employees are not permitted to set up for personal use groups, blogs or any other form of social media which is HPC branded, contains content for which the HPC owns the copyright or which could be linked with the HPC.

4.9 HPC employees are not permitted to use their HPC email address for personal usage, for example to set up social media networks.

## 5.0 Inappropriate use of social media

5.1 Inappropriate use of social media, for example making insulting or defamatory statements on social networking sites about the HPC, its employees, partners, registrants or any other stakeholders could result in serious complaints or legal claims being made against both the HPC and individual employees.

5.2 A breach of this policy may be regarded as either an act of misconduct or gross misconduct, depending on the seriousness and the effects of the breach. If an employee has breached this policy the HPC's Disciplinary procedure is likely to apply.

Appendix II

# Section 5h - Information Technology Policy

## 1.0 Purpose

1.1 The Information Technology policy is to set out the behaviour expected of users of the HPC's electronic information and communication technology systems and related equipment. This policy applies to all those persons accessing any systems provided by HPC.

1.2 The HPC encourages the use of its systems to aid communication and improve efficiency and working practices and those systems are critical to the efficiency of the HPC. However, inappropriate use of those systems can cause serious problems that may involve legal claims against both the HPC and against individual users.

1.3 This policy deals mainly with the use (and misuse) of computer equipment, email, internet connection, telephones, fax machines, copiers, scanners, and voicemail (collectively referred to as "systems") and sets out the standards that users of the HPC's systems are expected to observe.

1.4 Individuals using the HPC's systems are required to maintain standards of honesty and integrity at all times and to use only authorised access to the systems. The HPC will monitor use of these systems and will take action in respect of breaches of these standards.

## 2.0 Legislative Framework

2.1 Use by users of the HPC's Systems and monitoring by the HPC of those systems is likely to involve the processing of personal data and is therefore regulated by the Data Protection Act 1998 together with the Employment Practices Data Protection Code, issued by the Information Commissioner. The HPC is also required to comply with the Regulation of Investigatory Powers Act 2000, and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

## 3.0 Implementation and Application of the Policy

3.1 You should immediately disclose any misuse of the HPC's systems to your manager or the Director of IT.

3.2 This policy applies to all individuals working for HPC at all levels

## 4.0 Ownership

4.1 The HPC's systems, including electronic mail, telephones and voicemail, are owned by the HPC and are to be used for the benefit of the HPC in connection with its business

4.2 All data, files or information that reside on the HPC's Systems or transmitted by and though those systems, including word processing files, email, voicemail messages, or database files etc, are and remain the sole property of the HPC and should be accessed only by those individuals who have a business need to do so. Nothing entered, retained or transmitted is or shall be deemed to be the individual or personal property of the author or worker.

## 5.0 Security and Passwords

5.1 You are responsible for the security of equipment allocated to you. If you are given access to email or to the internet you are responsible for the security of your terminal and, if leaving a terminal unattended or when leaving the office, you should log off or lock your computer to prevent unauthorised users accessing your computer in your absence.

5.2 Passwords are unique to each user and must be changed regularly to ensure confidentiality. Passwords remain confidential and must not be made available to anyone else. When changing your password you should adopt a password that does not use personal data.

5.3 If you are issued with a laptop please ensure that it is kept secure at all times.

## 6.0 Authorised Use

6.1 Personal use of the HPC's systems at any time is a privilege. The HPC reserves the right to withdraw permission for personal use at any time.

6.2 Unauthorised review, access, damage, modification, alteration or deletion of any existing System, program, file, document, data, message or other information contained in any system without authorisation, or other damage to any of the HPC's Systems, amount to improper uses of those systems and are violations of this Policy.

6.3 You should not use the HPC's systems for any illegal activity or for any activity that violates any other of our workplace policies or is inappropriate for the HPC.

6.4 Confidential Information is used and created on a regular basis, and should only be accessed, edited, stored or archived if part of your designated work related tasks. Always assume personal information is confidential. Seek advice if in doubt from your manager or the person responsible for Data Protection and Freedom of Information.

6.5 Confidential documents may be designated as such through the document management system.

6.6 You may be granted access, in connection with your job responsibilities, to various information, documents and materials that have been generated by the HPC or received from third parties. If you are granted such access, you are bound by an implied and express contractual duty to keep the information fully confidential.

## 7.0 Monitoring

7.1 For business reasons, and in order to perform various legal obligations in connection with its role as an employer, use of the systems and any personal use of them is continually monitored. Monitoring will only be carried to the extent permitted or required by law and as necessary and justifiable for business purposes.

7.2 We will monitor use of the systems for the below reasons (however this list is not exhaustive) to:

- ensure that the use of the email system or internet is legitimate and in accordance with this and other workplace policies;
- find lost messages or to retrieve messages lost due to computer failure;
- assist in the investigation of wrongful acts; or
- to comply with any legal obligation.

7.3 By your use of the systems, you acknowledge that the HPC can and does examine logs of your activity on any IT system.

7.4 The HPC reserves the right to access at any time any computer file, data file, log file, document, voicemail message, email message or mailboxes to maintain and protect the Systems for the benefit of the HPC

## 8.0 Acknowledgement of Monitoring

8.1 In order to ensure that users are aware that HPC can monitor their usage of IT systems, we ask you sign this policy upon commencement of using any of HPC's IT systems as an acknowledgement that you understand that your usage can and is being monitored.

## 9.0 Emails

9.1 At the HPC's discretion, users will be provided with HPC email accounts for work-related purposes. Minimal personal use at a reasonable level is allowed and if you use the email for personal use you are encouraged to do so before or after work hours, or in breaks.

9.2 Any email messages created, sent or received via HPC's systems (including personal emails) are and remain the HPC's property and the HPC reserves the right to access and disclose the contents of all such messages. Email messages may be disclosed in legal proceedings in the same way as paper documents.

9.3 The HPC also reserves the right not to transmit any email message and to block access to attachments to emails for the purpose of effective use of the system.

9.4 Users should bear in mind the following when using email:

- All external virus warning email messages should be notified immediately to the IT Department.
- Always store copies of important emails in the HPC iExtensions system or save as an attached document in the registrations or FTP system
- You should not include material that anyone might consider offensive, such as sexist or racist remarks.
- You should not use email in any way as part of private commercial business.

**10.0 Internet Access**

10.1 The HPC, at its sole discretion, may provide you with access to the internet by way of the HPC's Systems. You may only access the internet by using the HPC's software, firewall and router. The HPC may block or restrict access to websites or webpages at its sole discretion.

10.2 If you are granted access to the internet for business purposes:

- Your browser should only be left open on www.hpc-uk.org or webpages therein even if minimised.
- Personal use of the internet should be kept be a minimum, reasonable level, and be occasional in nature. For personal use, employees are encouraged to use their lunch breaks or before and after work hours. Users who appear to spend a significant amount of time on the internet can be monitored.
- Editing or deletion of log files relating to internet access is forbidden.

10.3 Use of the systems to access inappropriate internet sites or to access sites that would violate any workplace policy is not allowable. As a general rule, if any person within the HPC (whether intended to view the page or not) might be offended by the contents of the page, or if the fact that the HPC's software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

**11.0 Personal Data Assistants and data stores.**

11.1 Only Personal Data Assistants (PDA's) provided by the HPC IT department are to be connected to the HPC network and used to store or process HPC information. No personally owned devices are to be connected to the HPC network or infrastructure.

11.2 All data and information transferred from the Systems onto a PDA will remain the property of the HPC. This also includes any data stores such

as USB flash drives, MP3 or similar device, floppy disk, cd or dvd, SIM card or telephone.

## 12.0 Telephone Calls

12.1 Personal telephone calls to or from the HPC's office or mobile telephones should be kept to a reasonable amount.

12.2 Users of HPC's telephone systems, including mobiles, should note that all calls are itemised. Non HPC business calls and text messages may be charged to you.

12.3 The HPC reserves the right to monitor, and/or record, telephone and voicemail communications, including for the purpose of determining whether business related messages have been received during your absence from the office. The HPC intends to exercise its right to monitor and record any telephone and voicemail communication for the following purposes:

- To investigate or detect unauthorised use of the telephone system
- To ascertain correct and acceptable standards of service are maintained
- To prevent or detect crime
- To ensure that the system is operating effectively
- To establish the existence of facts relevant to the business.
- To ensure compliance with regulatory or self-regulatory practices or procedures relevant to the HPC's business

12.4 Telephone and voicemail communications may be used as evidence in disciplinary proceedings or for any other legitimate purpose as required by the HPC.

12.5 At the HPC's discretion it will provide mobile telephones to certain users to assist them in performing their duties. Any mobile telephones provided to users will remain the property of the HPC.

## 13.0 Copyright Issues

13.1 Materials in websites or other external systems or email messages and attachments that you receive, may contain intellectual property belonging to others (including copyright, trade secrets or trademarked information). Users may not use the systems in ways that infringe any party's copyright or related rights. This is because violations of copyright (or other similar rights) may subject you and the HPC to civil and/or criminal penalties.

13.2 As a general rule, you may not forward, distribute or incorporate into another work material received from a website or other external system. This includes music or other content on the internet. Reasonable use may be permitted in certain circumstances.

## 14.0 Security and Software

14.1 You should not delete, destroy or modify existing Systems, programs, information or data installed on the HPC's Systems. You should also not

attempt to gain access to restricted areas of the network or to any password-protected information, unless specifically authorised to do so.

14.2 You must not install or download software from external sources without authorisation from the IT Department. This includes programs, instant messaging programs, screensavers, graphics, files, cartoons, photos, video clips and music files.

14.3 Users cannot access external instant messaging technologies.

14.4 Users must not deliberately introduce computer viruses to the HPC's computer system. The IT Department should be notified immediately if a suspected virus is received. The HPC reserves the right to block attachments to emails for the purpose of effective use of the system and reserves the right not to transmit any email message to its intended recipient.

14.5 The unauthorised copying of any copyrighted material, including programs, off of or onto the HPC's systems, is prohibited. . HPC mobile IT equipment must not be used wirelessly or wi-fi enabled for security reasons, other than where an HPC 3G card and VPN is used as the connection mechanism.

## 15.0 Crime and Data Protection

15.1 The Computer Misuse Act makes unauthorised access to, or modification of, computer held software or data a criminal offence. It is therefore important that everyone who works for the HPC has a clear understanding of what they are, and what they are not, allowed to do with the HPC's systems. It is the HPC's policy to comply with all laws regulating computers and data protection. It is therefore important that you limit exposure to risk through careless practices with regard to the use of data or inappropriate or illegal use of software.

15.2 You are only authorised to use systems and have access to information that is relevant to your job. You should neither seek information nor use the systems outside of this criterion.

15.3 Any mobile IT equipment (such as laptops, mobile phones, PDAs) in your possession containing any type of sensitive, personal or private data should be transported, used and stored securely in order to limit loss, theft and unauthorised data access. Such equipment should be securely locked and protected by a password in order to limit unauthorised data access.

15.4 Most of the information stored on the Systems relates to individuals, such as the HPC's registrants, applicants or users. As such, that information is deemed to be sensitive and must be protected to the best of your and the HPC's ability. Access to this type of information must be strictly controlled. You should not distribute personal information to external organisations or individuals without the prior consent of the individual in question and no information should be distributed if doing so would infringe data protection provisions.

## 16.0 Examples of Inappropriate Use

16.1 As misuse of the HPC's technologies can result in serious consequences for users and in some cases, referral to the disciplinary, it may be helpful to outline some examples of what may be considered inappropriate.

- Pornographic material (including writings, pictures, films, or video clips of a sexually explicit nature)
- Offensive, obscene or criminal material or material which is likely to cause embarrassment to the HPC, its members, officers or users
- False and defamatory statements about any person or organisation
- Material which is discriminatory, offensive, derogatory or may cause embarrassment to others
- Confidential information about the HPC and any of its registrants, applicants, members or users
- Any statement which is likely to create a liability (whether criminal or civil) for you and/or for the HPC
- Material breach of copyright
- Online gambling

## 17.0 Agreement

By accepting employment with and by continuing to be employed by the HPC confirms that you understand and agree to comply with the terms of this policy.