



**Isle of Man  
Government**

*Reiltys Ellan Vannin*



# Electronic Communications and Social Media: Policy, Standards and Guidelines

September 2015

## **INTRODUCTION**

The Isle of Man Government embraces innovation, and is committed to 'using technology to support better delivery of services and reduce bureaucracy' as outlined in its Agenda for Change.

As a result, Government is striving to improve the way it shares information and interacts with its customers and the community it serves. Electronic communications and social media which open up many new and exciting opportunities have a role to play in that process. It is important, however, that we use this technology responsibly and sensibly to avoid reputational harm to individuals or the organisation, as a whole.

This Policy, Standards and Guidelines document provides employees with information concerning their rights and responsibilities in relation to the use or development of any electronic communication or social media application. It aims to help employees achieve the best from the tools available whilst maintaining a safe professional environment and protecting themselves, as well as the Government.

The Electronic Communications and Social Media Policy, Standards and Guidelines have received the endorsement of the Council of Ministers, with the support of the Chief Officers Group, and relate to all Isle of Man Government employees.

**Allan Bell MHK**  
**Chief Minister**

**September 2015**

# INDEX

Policy .....	4
1. Policy Statement .....	4
2. General Statement.....	4
3. Scope and Coverage.....	5
4. Monitoring .....	5
Minimum Standards .....	7
1. Minimum Standards for all users when using all forms of Electronic Communications and Social Media .....	7
2. Standards to follow when using Social Media as an Individual .....	8
3. Standards to follow when using Social Media as part of your Job or posting to a Government Channel.....	8
Guidelines.....	10
1. Guidelines to follow when using Social Media as an Individual.....	10
2. Guidelines to follow when using Social Media as part of your Job.....	11
3. Summary.....	11
4. Security, Safety and Privacy tips for anyone using Social Media .....	12
Additional Resources and Policies.....	13

# Policy & Guidelines for the use of Electronic Communications and Social Media

## Policy

### 1. Policy Statement

The Isle of Man Government recognises the important role that electronic communications and social media play in creating a culture of working that is responsive, effective and flexible. Government actively encourages users to engage with all forms of electronic communication and social media and exploit the benefits that these technologies offer, for example promoting the provision of services, informing users of service development, answering enquiries and receiving feedback from customers. However it is also important that users are mindful of the potential risks involved, both to themselves and the Government, and to ensure that they use all forms of electronic communication and social media safely, responsibly and legally.

It is Government policy to ensure privacy, confidentiality, and security in electronic communications, to meet its legal and statutory obligations, and to protect the reputation of Government. Recent case law would indicate that there is no right to privacy when using social media as an individual and the lines between work and home life can become very blurred. It is important that users of electronic communications and social media recognise this.

In support of this Policy, Standards and Guidelines, Isle of Man Government will communicate the required standards and behaviours expected from all users of Government electronic communications equipment, such as but not limited to e-mail, internet, social media (including but not limited to blogs, social networking, wikis, forums, message boards etc), telephone and work voice-mail facilities. Isle of Man Government reserve the right to monitor the use of e-mail, internet, social and media networking, telephone and voice-mail facilities to ensure compliance with this Policy, Standards and Guidelines and related procedures.

### 2. General Statement

The guidelines and examples provided are not exhaustive and may differ slightly from Department to Department, depending on operational requirements. However, it is suggested that as a general rule, individuals are mindful that they should not put into electronic or social media format anything that they would not be prepared to state verbally or in writing or print and have attributed to them. Users are expected to take a reasonable and common sense approach to their use of these media, in respect of both how they use them as well as how much. The principles within this document should also be borne in mind by users when they engage with electronic or social media in their personal time, especially where they can be identified as a member of staff.

This Policy, Standards and Guidelines document is intended to protect the security and reputation of the Isle of Man Government and that of the employing Department or Board. It is recognised that there needs to be a balance between the considerable benefits of electronic communications and social media for Isle of Man Government and its staff, and the potential risks that may arise through lack of understanding or training. When users are fully aware of this, they can use the media more effectively.

This document should also be read in conjunction with the Public Service Code of Conduct, Government Information Security Policy and Data Protection Policy. It is also suggested that users familiarise themselves with the Disciplinary Policy relevant to their terms and conditions of employment, as well as the Fairness at Work Policy, which set out standards of behaviour that are

acceptable, the implications for a breach of the minimum standards, as well as what course of action is available to individuals who may find themselves in conflict.

### **3. Scope and Coverage**

This Policy, Standards and Guidelines applies to all users who have access to the Isle of Man Government<sup>1</sup> electronic communications systems, Government devices and personal devices, enabled to do so, when they are connected to the Government network. This includes all individuals whether employed on a permanent, part-time, temporary or locum basis, as well as third party and contract staff. The Policy, Standards and Guidelines also applies to users engaging with electronic or social media in a personal capacity, outside of their normal place or hours of work.

What, where and how content is published is important, particularly now that the lines between public and private, personal and professional life are becoming increasingly blurred. What is published online in a personal context can easily be associated with Isle of Man Government and this Policy, Standards and Guidelines are to help users protect and promote Isle of Man Government and themselves online.

This document is not intended to replace guidance provided by Professional or Registration Bodies (for example the Law Society, General Medical Council, Nursing and Midwifery Council, Royal Institute of British Architects etc). Individuals who are members of these bodies must ensure they are also aware of and compliant with their guidance on social and electronic media.

All elected members are to be made fully aware of the Policy, Standards and Guidelines and of their responsibility to ensure privacy, confidentiality, security and appropriate use of electronic communications.

Where appropriate the Policy, Standards and Guidelines should also be communicated externally, e.g. to contractors etc.

This Policy, Standards and Guidelines document, and associated guidance, replaces the following documents:

- Electronic Communications – Email & Internet – Minimum Standards
- Electronic Communications – Inappropriate Use
- Electronic Communications – Acceptable Use Policy

Breach of the minimum standards within this document may be dealt with under the Disciplinary Policy relevant to the terms and conditions of employment and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

There are Policies and Procedures in place through which staff can raise concerns and 'let off steam', for example Confidential Reporting (Whistleblowing) or the Grievance procedures and Fairness At Work Policy.

### **4. Monitoring**

Government resources, including e-mail, internet, social media, telephones and voice-mail are provided for business purposes. Therefore the Isle of Man Government reserves the right to monitor the legitimate use of these business facilities.

---

<sup>1</sup> For the purposes of this document "Isle of Man Government" or "Government" is taken to mean all 'designated bodies' as defined within the Financial Regulations.

The monitoring or recording of e-mail and voice-mail messages and use of internet, social media and telephone facilities will only be undertaken for the following, specific, legitimate business purposes:-

- to ascertain compliance with regulations, Policy and procedures;
- to investigate or detect unauthorised use of business systems;
- to ensure the effective operation of those systems; and to prevent or detect crime.

# Minimum Standards

## Minimum Standards for the use of Electronic Communications and Social Media

The Isle of Man Government has developed a set of minimum Standards that must be adhered to by all users who engage with electronic communications and social media, whether privately or in a work capacity. Failure to adhere to one or more of these Standards may result in disciplinary action and potential dismissal.

Users should be aware that all information<sup>2</sup> that they hold or create may be the subject of a Freedom of Information or Subject Access request. This may include Government or personal email accounts and mobile telephones where these have been used for official business. It is strongly recommended that users acquaint themselves with the provisions of this legislation.

Where there is any doubt, it is strongly advised that individuals or Department representatives contact Government Technology Services or the Office of Human Resources for further advice.

### 1. Minimum Standards for all users when using all forms of Electronic Communications and Social Media

The following activities are expressly forbidden, and a deliberate act in relation to any of these activities may be regarded as misconduct and in serious cases could result in dismissal from employment:-

#### Unauthorised Use:

1. The intentional introduction or attempted introduction to Government of any form of Trojan, computer virus or other malicious program.
2. A deliberate attempt to gain unauthorised access to restricted areas of the network through the use of "hacking" and/or other unauthorised activities.
3. Forgery and/or attempts to read another Government user's electronic communication without their express permission.
4. The automatic redirection of e-mail to external e-mail accounts without express permission.
5. Disclosing or allowing anyone else to use your user name and password to gain unauthorised access to any of the Government's systems.
6. Transmitting, receiving, copying or storing digital media (including software, music, video etc.) except for reasonable personal use (for example personal photographs) and legitimate business purposes which comply with the copyright and licensing regulations.
7. Playing computer games, accessing chat rooms or similar personal entertainment to the detriment of their role or Government reputation.
8. The encouragement or promotion of activities, which may be an unproductive use of Government resources. Possible examples include the inappropriate distribution of unsolicited messages e.g. chain letters, junk mail and jokes.
9. Uploading or downloading (or attempting to download), using, retaining, distributing or disseminating any images, text, materials or software onto, from or with a Government computer which would be a breach of copyright or license provision with respect to both programs and data.

---

<sup>2</sup> 'Information', for the purposes of the Freedom of Information Act 2015 and the Data Protection Act 2002, covers any printed or electronic files, sound and video recordings as well as drafts and hand written notes.

### **Activities that Damage the Government:**

1. Any activity which could compromise the legal, regulatory or contractual obligations of Government, could breach the confidentiality of information or could have negative repercussions on the reputation of Government.
2. Ensure that personal opinions are not attributed to the Government or Departments.

### **Activities that Damage Relationships:**

1. Making derogatory, defamatory or malicious remarks or expressing derogatory opinions about the Government or staff working within Government. It is recommended that users familiarise themselves with the Bullying and Harassment Policy / Fairness At Work Policy, which outlines the behaviours that are expected of Government staff.
2. 'Trolling' i.e. making deliberately offensive, inflammatory or contentious statements online with the intention of inciting a reaction.
3. Knowingly infringing copyright or intellectual property rights. Copyright arises when an individual or company creates a work, and gives the owner or creator control over how it is broadcast, copied, adapted, issued, rented and lent. It is an offense to copy, share, lend or issue, perform or broadcast, or adapt the work without the consent of the owner.
4. Uploading or downloading (or attempting to download), using, retaining, distributing or disseminating any images, text, audio recordings, materials or software which:
  - a) are or might be objectively considered to be indecent, obscene, pornographic<sup>3</sup>, or are or might objectively be considered to be violent, distasteful and alarming, or an incitement to criminal or illegal behaviour. (If you receive an electronic communication of this nature, you must promptly notify your line manager or another appropriate manager or supervisor);
  - b) are or might be objectively considered offensive or abusive, in that its context is or could be considered to be a personal attack, rude, sexist, racist or generally distasteful. (If you receive an electronic communication of this nature, you must promptly notify your line manager or supervisor);
  - c) users cannot or are not prepared to be accountable for.

## **2. Standards to follow when using Social Media as an Individual**

### **Minimum Standards for all Users**

#### **Do not:**

1. Use the Isle of Man Government crest or identity to endorse personal opinions or viewpoints.
2. Use Social Media to 'Whistleblow'. The 'Confidential Reporting (Whistleblowing)' Policy outlines the process to follow if you have concerns about your workplace.
3. Post comments or images which are abusive, improper or offensive or which could be construed as bullying, harassment, victimisation or 'trolling'.
4. Post comments or images which could be portrayed as committing an offence or anti-social behaviour, or that brings the Isle of Man Government into disrepute.
5. Post confidential information relating to Isle of Man Government or its staff online.

## **3. Standards to follow when using Social Media as part of your Job or posting to a Government Channel**

### **Minimum Standards for Use of Social Media for all Users**

1. Seek approval from the appropriate Manager or Accounting Officer if the use of social media and / or the creation of a social media presence (accounts, pages, groups, events etc) is not already expressly provided for in your job description or consider requesting an amendment to your job description to reflect your responsibilities.

---

<sup>3</sup> Government defines indecent, obscene and pornographic material as the description or depiction of sexual acts or of a sexual nature.



2. Do not give personal opinions that could bring the organisation into disrepute.
3. Do not detail religious or political beliefs.
4. Your use of Social Media should be relevant to your role.
5. Where your use of social media is identifiable as being by a Government official or from a Government account do not 'like' other individuals' or bodies' pages/sites or provide links to them unless to be associated with the content is wholly consistent with department policy or otherwise approved by the Chief Executive. Any 'liked' or linked pages must be monitored to ensure that changes do not make that cease to be appropriate. ('Liking' may be construed as formal endorsement by the department.)

# Guidelines

## Guidelines for the use of Electronic Communications and Social Media

It is recognised that a clear and comprehensive set of guidelines and recommendations on best practice can also assist users to make full use of the potentials offered by electronic communications and social media, whilst protecting themselves, their Department and the Isle of Man Government. It is strongly recommended that users acquaint themselves with these guidelines, which are intended to minimise the risks posed by using electronic communications and social media and avoid any potential consequential disciplinary action.

Individual Departments or Boards may find that certain behaviours are of greater or lesser seriousness, depending on that Department or Board's functions and accountabilities and may vary these guidelines accordingly.

Likewise, individual Departments will have individual ways of maximising the benefits electronic communication and social media, depending on their business needs.

A handbook that you may find useful, entitled 'Guidelines for the Use of Electronic Communications and Social Media' is available [here](#).

### 1. Guidelines to follow when using Social Media as an Individual

#### Guidelines

1. Think before you post.
2. Be honest and truthful.
3. Take steps to protect Personal Data such as date of birth, address etc.
4. Avoid using your official Government email address when accessing online services and social media for personal use.
5. Ask whether it passes the Publicity Test – would you be happy to have your statement attributed to you in the national media?
6. Be respectful of others.
7. Monitor comments.
8. Set security to restrict access/visibility to friends only.
9. Be selective with 'Friends' as well as what you 'Like', 'Share', 'Retweet' etc on Social Media as associating yourself with a particular post, particularly one that may denigrate Government or its staff, may be deemed to be an endorsement of that post.
10. Ensure you comply with the Terms of Use of any Social Media platform you are using.
11. If you post about any aspect of your work as a public servant or your colleagues, even from your personal account, be mindful of the content and your audience.
12. Don't use pseudonyms.
13. Reasonable use of classified ad forums, such as the Government Buy and Sell page, Manx.net classified etc, should be conducted within your own time.
14. Be aware that anything posted online may exist in perpetuity: for anything you post, ask yourself if you will be comfortable with it resurfacing, possibly unexpectedly, some time in the future.

## 2. Guidelines to follow when using Social Media as part of your Job

### Guidelines

1. Think before you post.
2. Ensure you are familiar with this Policy, Standards and Guidelines document.
3. Ensure you are accurate.
4. Ensure you are timely.
5. Be responsible.
6. Respect others.
7. Be thoughtful.
8. Be yourself but adopt any defined or desired Department style if required.
9. Be personable not personal.
10. Be polite, impartial, clear and transparent.
11. When possible, it is generally desirable to maintain regular posts to keep followers engaged.
12. Remember why you are posting - keep posts relevant to your role.
13. Link to other government sites and partner agency sites. Where your use of social media is identifiable as being by a Government official or from a Government account do not 'like' other individuals' or bodies' pages/sites or provide links to them unless to be associated with the content is wholly consistent with department policy or otherwise approved by the Chief Executive. Any 'liked' or linked pages must be monitored to ensure that changes do not make that cease to be appropriate. ('Liking' may be construed as formal endorsement by the department).
14. Use Social Media when appropriate, not to the detriment of more pressing workload.
15. Use appropriate language.
16. Monitor and respond to comments on your posts.
17. Direct any complaints received via Social Media to the appropriate channels or person.
18. Don't be drawn into or escalate heated discussions. Stick to the facts and keep your tone professional at all times.
19. Don't discuss any third parties without their prior knowledge or consent.
20. Be careful how you link personal and work accounts.
21. Provide appropriate opinion / updates / comments on ongoing work issues / projects.
22. Don't re-tweet personal posts.

### 3. Summary

#### As a general rule, remember:

- If you are in doubt – ask before posting.
- Why you are posting – to share public information, not for personal betterment.
- To think before you Re-tweet or Share another post, comment or image.
- What appears 'light hearted' to you may offend others.
- To keep your **work** and **personal** posting completely separate.
- Don't use information that you obtain during the course of your normal work to inform what you post online – maintain confidentiality.
- What is 'done' cannot be 'undone' - once it's posted then it's there forever.
- What you post is disclosable.
- Respect copyright.
- Check spelling and grammar before you post.
- Comply with the law

#### **4. Security, Safety and Privacy tips for anyone using Social Media**

The internet is open to a world-wide audience. When using social media channels, consideration should be given to the following:

- Privacy settings to help control who can view user profiles, personal information and photos. Access to this information cannot be completely controlled, and users have no control over what someone else may share.
- How much information to impart. How may information such as phone number, address, car registration, a list of possessions be used if it is shared? With whom will the information be shared? Not everyone will respect personal or physical space.
- The image that materials and images shared on social media can project to potential employers, the general public, family members etc. Inappropriate material can create a negative image, which may have further consequences for career advancement, or work relationships.
- Removing material that has been posted thoughtlessly can be difficult. Posted material can remain accessible on the internet until the prescribed process for removing information from the caching technology of one or multiple (potentially unknown) search engines has been completed. This can be lengthy and difficult to do.
- Posting images or information about others without their consent can infringe their privacy and may lead to legal action in extreme cases.
- Some sites may render users vulnerable to computer viruses and SPAM or other unsolicited communication. Viruses can destroy data and infect other users. It is recommended that information is backed up to an external source in case of destructive attacks.

## **Additional Resources and Policies**

Public Service Code of Conduct

Fairness at Work Policy and Guidance

Government Information Policy

Data Protection Policy

Confidential Reporting (Whistleblowing) Policy

Relevant Employing Authorities' Disciplinary Policies



This document can be provided in large print or as an audio recording on request

Office of Human Resources  
2nd Floor, St. Andrew's House,  
Finch Road, Douglas, Isle of Man, IM1 2PX