
An Garda Síochána



Guidelines to Garda Staff on the Use of Social Media

March, 2014

Table of Contents

1.	Introduction	2
2.	Policy Justification	3
3.	Private Capacity	3
4.	Supervision	3
5.	Monitoring	4
6.	Examination by Garda Professional Standards Unit	4
7.	Awareness Raising	4
8.	Information Technology Support	4
9.	Discipline	4



1. Introduction

The purpose of this guideline document is to instruct all Garda *members* and civilian personnel in An Garda Síochána (hereinafter referred to as Garda staff) regarding the 'Use of Social Networking Sites'. It should be read in conjunction with HQ Directive 35/12 on 'Internet & Electronic Mail Policy - Version 3'.

In modern times the use of information technology fora on the internet, such as blogs, message-boards, social-networking and e-mail communications, has provided An Garda Síochána with many opportunities and challenges. Indeed, the introduction of advanced IT systems, such as PULSE, GARDAIS and the Garda website, has undoubtedly increased the capacity of An Garda Síochána to deliver a professional policing service to our communities.

Social-networking sites and web-based fora, such as *Facebook*, *Bebo*, *Twitter* and *YouTube*, provide individuals and groups infinite on-line opportunities for global communications and networking. An Garda Síochána has embraced the social-networking concept of communications. The Garda Press and Public Relations Office recently established an official *Facebook* page, with a view to ensuring that An Garda Síochána reaches an even wider target audience.

An Garda Síochána recognises that Garda staff, in their private capacity, may use social-media as a pastime or hobby and as a form of communicating with family, friends or relatives. However, Garda staff, in the context of their job, hold a unique and critical security and safety role within Ireland. This policy is designed to provide advice and information for Garda staff to be mindful of when using these fora. Critically, this Policy also clearly sets out the boundaries for Garda staff when using social-media, in order to ensure safety and security of Garda staff, the public, and to minimise risk to the corporate image and reputation of An Garda Síochána. Breach of this Policy may result in disciplinary action being taken and, in this regard, a number of prohibitions are clearly set out *at paragraph 5 of the HQ Directive*.

This Policy was developed following exhaustive research and consultation process and implementation will be supported and monitored through various awareness-raising and auditing structures.



2. Policy Justification

The justification for the introduction of this Policy is to : -

- ✓ Reduce risks to Garda operations and the corporate and reputational image of An Garda Síochána
- ✓ Meet legal obligations contained within the *Official Secrets Act, 1963*; the *Garda Síochána Act, 2005*; and the *Data Protection Acts, 2003 and 2008*
- ✓ Ensure the safety and security of Garda staff, their colleagues, families, relatives or friends and the general public, and
- ✓ Ensure the delivery of a professional, impartial and human-rights compliant Garda service.

3. Private Capacity

An Garda Síochána recognises that Garda staff, in their own, private, capacity, may wish to view or publish comment on the internet, for example in blogs, message-boards or on social-networking sites, similar to *Facebook*, *Bebo* or *Twitter*. Such activities are, however, **prohibited** while using any Garda IT and Telecommunication systems, unless specifically required and approved, for operational reasons.

All Garda staff who upload or publish comment on the Internet, are strongly advised to be mindful of the implications of providing written, vocal or visual information which identifies, or could identify, themselves or others, as a member of Garda staff.

Internet fora are subject to ‘hacking’ and can, potentially, be screened / monitored by criminal elements for their own ‘intelligence-gathering’ purposes. All Garda staff shall ensure that any comment which they up-load / post on the internet does not pose a security or safety risk to themselves, their colleagues, family, friends, the public and does not compromise Garda operations or the corporate image and reputation of An Garda Síochána.

4. Supervision

Supervisory first-line managers will ensure that the contents of this Policy are brought to the attention of all their respective Garda staff. Each Chief Superintendent / Principal Officer will forward a return in writing, to their respective Assistant Commissioner /



Executive Director / Director, certifying that each Garda staff member in their division / area is aware of the content of this Policy and accompanying HQ Directive.

5. Monitoring

This Policy will be monitored by Garda Internal Affairs Section. Supervisors should ensure that this issue is regularly addressed as part of briefings and accountability meetings. In addition, Garda staff should report, through appropriate channels, items / entries on social-media they become aware of which may breach the terms of this Policy.

6. Examination by Garda Professional Standards Unit

Adherence to this Policy will be examined by the Garda Professional Standards Unit.

7. Awareness Raising

Awareness raising of this Policy will be supported through :

- ✓ inclusion of a HQ Directive and accompanying Policy on the Garda Portal;
- ✓ a 'splash-screen' image on every PC;
- ✓ circulation of an 'information leaflet' and posters to all Garda stations and buildings;
and
- ✓ promotion of social-networking safety via the Garda Portal

8. Information Technology Support

Garda staff who have uploaded or published comments / entries on the internet / social-networking sites which contravenes this Policy will immediately remove it. If unable to do so they shall report same, without delay, through the appropriate channels, to the Executive Director, ICT.

9 Discipline

Any breach of this Policy will be taken very seriously and may result in disciplinary action being taken.

