Council of the European Union
General Secretariat
Directorate-General Administration
Directorate-General Communication and Document Management

STAFF NOTE
CP 35/15
Brussels, 2 June 2015

Subject: **GSC Social Media Code of Conduct**

This Staff Note concerns all staff.

The GSC recognises that social media is an increasingly used tool in the private and professional lives of GSC staff.

The Social Media Code of Conduct accordingly provides advice for using social media. To help staff, a single point of contact for advice or suggestions related to social media has been created. All questions and comments should be addressed to the Social Media Infodesk at social.media.infodesk@consilium.europa.eu.

Please be aware that the use of some social collaboration platforms, such as Yammer, is currently not approved for professional use by GSC staff neither internally nor for collaboration with users outside the GSC. The GSC is working with other institutions to address this need in a suitable way.

This staff note replaces and repeals Staff Note 88/11.

William SHAPCOTT
Director-General

Reijo KEMPPINEN
Director-General

GSC'S SOCIAL MEDIA CODE OF CONDUCT

Purpose of this Code of Conduct

1. This code of conduct explains how GSC staff can use social media in an appropriate, safe and legally sound way consistent with the values expressed in the GSC mission statement and in line with the Staff Regulations and the GSC Guide to Ethics and Conduct. The advice in this document helps protect the security of GSC networks, the GSC's reputation and the privacy of its staff.

2. Social media can be used in two capacities: **private**, you as an individual in your private life, and **professional**, either an identifiable GSC employee in a work-related capacity or managing a corporate account on behalf of the GSC. Part A of these guidelines outlines the good practice that you should employ when you use social media. Part B gives additional information and guidance to staff who administer or use Council social media channels or who are asked to participate in social media as part of their professional activities.

3. These guidelines apply to all GSC staff. They should be read in conjunction with the IOLAN Code of Practice[1].

4. For advice and guidance on social media related matters, unless indicated otherwise, please send your questions, suggestions or comments to the Social Media Infodesk - *social.media.infodesk@consilium.europa.eu*. Security-related incidents (e.g. sensitive or internal Council matters divulged on social media) should always only be reported through SIRA (security incident reporting and recording application) on DOMUS.

[1] CP 92/2014.

General Background

What are social media and how does the Council use them?

5. Social media are online platforms that enable individuals and organisations to easily create and share content. Social media encourage two-way communication and engagement such as participating, discussing, sharing, networking, collaborating and bookmarking online. Social media can take many forms including micro-blogs, forums, customer review sites, search and discovery services, sports activities and location services, bulletin boards, photo and video sites, fun or professional networking sites, messaging applications collaborative platforms, social games and virtual worlds.

6. Social media are very often offered at no financial cost to you. However, be aware that according to the business model of social media, you are the 'commodity' and not the customer of social media services. Data about you, your usage of social media and people and activities related to you are sold on by social media companies to their customers.

7. The Council currently uses several social media platforms as part of its overall external online communications and public relations efforts. These platforms are managed by DGF and run by GSC staff with expertise in the field. Council social media are subject to a centrally coordinated content calendar, visual identity and overall communication strategy.

8. The GSC recognises that social media are changing the way people work, communicate and socialise. Increasingly, social media are used for professional purposes in business and government. They can also be used to support the way in which GSC staff stay informed, follow developments either in the news or in a particular field of knowledge and policy development, or collaborate. Social media have many positive attributes, but by using them, it is also possible to create negative or unintended consequences for people and organisations.

Why you should consider communication through social media as enduring and public

9. Regardless of your privacy settings, when you use social media in either a private or professional capacity, you should consider that all information shared is enduring and public. By public, we mean that information in most social media platforms is made accessible by the service providers to other users. Information can also easily be forwarded or re-transmitted to a wider audience than you intended, for example by friends who share your social media updates. By enduring, we mean that anything you put on social media, even if it is deleted immediately, is likely to be available and retrievable indefinitely. Once information is shared, neither you nor the GSC has full control over it.

Social media and security

10. There are risks to you and the institution through using social media that you should be aware of. It is important to conduct yourself in a safe and legal way on social media and to be aware that your reputation and that of the GSC could be adversely affected by your conduct. Your posts and activity on social media platforms can be used to determine your location, associations, habits and other personal data about you. Social media also present an attractive for malicious code (malware) to spread. The Security Office is aware of cases where private or sensitive data posted on social media have been exploited by foreign intelligence services.

11. The GSC may take action to limit access to some sites and services from its networks for security reasons or if the GSC networks or their functioning are at risk[2].

GSC staff's use of social media

12. You may make reasonable private use of social media websites from GSC computers or devices provided this does not interfere with your professional responsibilities nor interfere with the smooth running of the GSC.

13. In principle, you may access and use social media in direct support of your **professional** activities using your professional email.

[2] See CP 97/2011.

14. You must not use your GSC email credentials for **private** use of social media, and **never** re-use your GSC passwords for any social media accounts.

15. Whenever you use social media, you are still bound by the Staff Regulations. The line between private and professional use is not clear-cut. We create perceptions about ourselves as professionals, as individuals and the GSC as an organisation when we use social media in a way which is traceable to our professional duties.

16. You are free to express your own opinion but you should make clear that it is your opinion and not an official view or position of the GSC. You could add a disclaimer to your user profile, similar to the use of disclaimers in emails sent from GSC email accounts. For more guidance, please check with the Social Media Infodesk.

17. You can use social media for monitoring or information gathering purposes as part of your job. In many cases it is possible, often advisable, to do this passively - i.e. without being active on a social media platform yourself. In some cases you do not even need to sign up (for example, Twitter).

PART A:

18. Good practice to help you be more secure:

    a) **Minimise the availability of your personal data**
    When you interact on social media, be aware that the information you share about your work, yourself, your colleagues and your family can be used by people who seek this type of information with the intent to cause harm to the Council's interests, to you, your family, colleagues or the GSC. Keeping the amount of data you list in your profile and your relationships to a minimum reduces the risk that such information can be misused or exploited.

b) **Clear old history and consider risks before posting**

Remember that what you share with friends and contacts online may also be shared by them and what you contribute to social media may quickly get out of your control as information can be shared or re-transmitted without your knowledge. Be aware that your 'historic' posts in social media which may pre-date your current employment, are still searchable and could be a potential source of embarrassment. This could negatively affect your reputation as well as that of the GSC. It is good practice to clear old history and to consider what you comment on or tag in the future.

c) **Avoid using geo-locational features**

You are strongly advised not to use geo-locational features such as 'checking-in' on social media and apps and to switch off location services (GPS) on your smart phone, unless you really need them for a specific app. Many sports-related apps encourage you to share personal data as well as routes and timings online. Geo-locational data can easily be used to track your movements and to reveal your routines and habits.

d) **Avoid disclosing your plans**

It is good practice not to reveal in advance what you are going to do and where you are going to go, including travel or mission plans (useful information for burglars and others), but you could share experience once the event has happened. We recognise that live tweeting during an event you attend or speak at is now common practice - be prudent with information that can give unnecessary additional information about your location.

e) **Do not disclose any security features or classified information**

Never disclose or share any classified information, LIMITE or GSC Internal information on any social media, even after leaving service. Do not mention anything about the security processes, procedures or equipment of the GSC, nor any internal work-related information that may be of interest to many people outside the GSC who do not need to know this information. Such security-related information in text or images may be used by activists and extremists to carry out actions that may harm the Council or the many people who use Council buildings on a daily basis.

f) **Privacy settings**

Unless you particularly wish to be easily identifiable, it is good practice for a personal social media account to make sure that the privacy settings are set high. This will limit your visibility but it is a safer option, as social media platforms no longer allow users to be completely anonymous.

g) **Safeguard personal contacts on mobile devices**

Be aware that if you use apps or games via social media, it is probable that your contacts and other information on your mobile device will be accessed by the apps/games as part of the terms and conditions of use. Before installing an app/game, consider if you really need it on your device.

h) **Separate sign-ins**

It is preferable to sign into social media using the official webpage and an existing account rather than using one singe social media account (such as Facebook, Google, Yahoo etc) to access another social media account such as LinkedIn. It is normal for social media to access large amounts of information about you and your contacts as part of a multiple sign-in process.

i) **Use a browser**

It is recommended that you log into social media sites such as Facebook via your browser rather than installing an app that may access your contacts and make suggestions to you or your contacts that you should link together using the app.

j) **Two-factor authentication**

Be aware that two-factor authentication, if available, provides an additional layer of security that requires a verification code to be entered in addition to your user name and password. The verification code is sent to you by your provider to a pre-arranged email address or number (sms or an automated voice message).

19. Good practice to help you stay legal and to protect privacy:

a) **Your obligations as a staff member**

Remember that you are bound by the obligations in the Staff Regulations, in particular Title II, Rights and Obligations of Officials, which stipulates that staff must, amongst other things, refrain from any action or behaviour that might reflect adversely upon your position. While the prior authorisation of the Appointing Authority is not required in principle before posting on social media platforms, you should apply your judgement within the context of the staff regulations before publishing. If you are uncertain, please consider contacting the Social Media Infodesk or the Appointing Authority (DGA1 Legal Advisors, unite.conseillers.dga1@consilium.europa.eu) in advance.

b) **Images and tags**

Respect 'image rights' and do not share or post images of colleagues without their permission. Please do not post photographs of sensitive or non-public parts of the GSC premises. Do not 'tag' colleagues in photographs or tag within comments or posts, other images, without the permission of the people in the photographs and do not share images that have geo-locational data.

c) **Avoid comments of an illegal or discriminatory nature**

Do not post illegal, inappropriate, discriminatory or defamatory comments about anyone. This will reflect negatively on you as well as the GSC as an organisation and could be the basis for legal action against you.

d) **Respect copyright law**

You should respect copyright law and make sure you have the correct permission prior to posting, sharing or distributing copyrighted materials. You are free to share posts/updates from official Council social media platforms.

e) **Pseudonyms (“fake” names)**

Be aware that even when using pseudonyms there are additional (generally hidden) data which could be exploited to determine your name and other relevant information about you.

20. Good practice to help you safeguard reputation:

a) **Consider dignity and reputation**

Consider the dignity, privacy and reputation of other people and organisations. We all have a part to play in managing our online reputation and that of others, including the GSC, regardless of whether we use social media in a professional or private context.

b) **Think before you post**

If you feel strongly about an issue and feel compelled to express your opinions on social media, take a break and consider the potential impact that your comments could have before you post something online. Show your comments to someone, preferably the Social Media Infodesk, before you upload them. Consider if you are the appropriate person to respond, especially if the post concerns the work and reputation of the GSC.

c) **If contacted by someone from outside the GSC**

If you are contacted by a lobbyist or journalist, please inform the Council's press office at *press.office@consilium.europa.eu* or phone ext. 6319. If you receive questions from the general public and are not sure if and how to answer, please contact the Social Media Info desk.

d) **Sometimes mistakes happen…**

If you think that you have made a mistake or an error of judgement, then please contact the Social Media Infodesk as soon as possible.

Don't ignore a potential mistake; the sooner it is addressed the easier it will be to reduce any negative impact. The Social Media Infodesk is here to help colleagues in a constructive way and to help find the best course of action.

PART B:

GSC corporate social media accounts

21. Official communication on social media happens through Council-branded social media accounts owned and managed by DGF. The rationale is that a centrally coordinated communication effort on social media is more successful in terms of reach and engagement. If you think that your unit or directorate has a business-related need for a presence on social media, then please contact the Social Media Infodesk to discuss your ideas. Please do not open independent Council-branded social media platforms. The Council's Social Media Infodesk welcomes opportunities for (regular) collaboration.

Use of social media in a personal-professional capacity

22. It is possible to use social media, for example Twitter, in an official capacity, provided that your job description and/or tasks support the use of social media. Current examples include Council press officers and some colleagues working in Cabinet positions. Such use requires the explicit approval of your line manager and has to be endorsed by the Council's press office. If you (would like to) use social media in this way, please contact the Social Media Infodesk to arrange a tailored session on security of information and other good practice.

Additional Guidance for a using Social Media in a professional capacity

23. When approved and in addition to the advice given in Part A:

    a) **Accuracy**
    Remember that you are responsible for the accuracy of the information that you post in your professional capacity. It is advisable to check that any links posted are working and point to the intended page(s).

    b) **Personality**
    Do not be afraid to inject/show your personality into your posts, but remember to stay professional at all times

c) **Enquiries and criticisms**

Refrain from any unsolicited or potentially provocative action. There are GSC services which are entrusted with the task of replying to citizens' queries or criticism against the EU or its institutions.

d) **Complaints**

Please report any social media complaints about an official GSC website to the Social Media Infodesk. A reply will be sent out from the Council's official social media accounts as soon as is practicably possible.