The Psychological Society of Ireland

Cumann Síceolaithe Éireann

The Psychological Society of Ireland Social Media Policy

Updated November 2018

Contents

1.0 Introduction

This Social Media Policy presents and explains the rules governing social media use at the Psychological Society of Ireland (PSI), including employees, Divisions and Interest Groups.

It follows that this Policy describes how designated staff members must use the company's social media accounts. It also explains the rules surrounding personal social media use during work hours and what employees may say about the PSI and company-related issues on their personal accounts.

With regard to PSI employees, this Policy must be read in conjunction with other PSI policies. Particular attention is drawn to the Email Etiquette Policy, which can be found in the PSI Governance Handbook, as well as the Code of Professional Ethics.

2.0 Why this Policy exists

This Social Media Policy exists to ensure employees, volunteers and members, regardless of their positions within the PSI, use their social media accounts in a safe and effective manner. Although social media can benefit the PSI — especially in terms of marketing, relationship building and prospect communication — poorly judged or timed activity may harm the Society's reputation.

2.1 Policy scope

The PSI Social Media Policy pertains to all staff members, members of the Society and volunteers, who log onto social media platforms during work hours or to complete PSI-related activities outside of standard PSI working hours.

By virtue of their position, each Chair of a Division/Interest Group has particular obligations with respect to general content posted on social media. They should consider whether personal thoughts published may be misunderstood as expressing the Society's opinion or position, even where disclaimers are used. Each Chair should err on the side of caution and should assume that their peers will read what is written. A public online forum is not the place to communicate organisation policies, strategies or opinions to members. Therefore, this Social Media Policy applies to all social media activity that relies on company Internet, occurs on company premises, happens while travelling and happens while working from home.

2.2 For the purposes of this Policy, social media may refer to:

- Popular social networks such as Twitter and Facebook.
- Photo-sharing websites such as Pinterest and Instagram.
- Video streaming websites such as YouTube and Vimeo.
- Professional social networks such as LinkedIn.
- Instant messengers such as WhatsApp and Facebook Messenger.
- Discussion forums such as those found on 4chan and Reddit.
- Question and answer-based networks such as Quora and Yahoo Answers.
- Review systems such as Yelp and Google Reviews.

Whether PSI employees, members of the Society and volunteers are posting from the Society's account or from personal accounts, they must follow basic practice guidelines.

2.3 Adhere to these standards to avoid common social media mistakes

Understand the social network. Different social media platforms have different purposes. For example, it is common to see more personal status updates on Facebook than LinkedIn. Before posting, become familiar with the network by reading FAQs and quickly researching what is and is not acceptable.

Correct your own mistakes. When you make a factual error in a post, create an update to correct it. Deleting or editing the original post should be at your own discretion, depending on the situation.

Be aware of potential security threats. Hackers can use social networks to distribute spam and malware. They can also launch phishing attempts. You should report suspicious activity, including questionable comments and friend requests to the service provider and to PSI at communications@psychologicalsociety.ie

Be careful when sharing information about yourself or others. Hackers can also use personal information to their advantage.

Do not escalate issues. Responding to other social media users, especially concerning a contentious subject, can result in a heated argument. To avoid such arguments, it may be best to avoid commenting if you feel you may cause conflict.

Think before posting. This is the golden social media rule. Not only should you check grammar and spelling, you should also ensure that a status update does not have the potential to cause conflict. Potential conflicts include creating arguments and divulging sensitive information.

2.4 General Data Protection Regulation (GDPR)

Though the GDPR policy is primarily aimed at EU citizens it also covers those who are in possession of EU-based personal data. The focus of GDPR is to ensure that consumers have rights such as:

- The right to erasure
- The right to restriction
- The right to object
- Information notices

GDPR classifies personal data as anything that can be used as part of identification. Beyond the obvious name, phone number, and address, this also includes:

- Bank information
- Photos

- Any numbers pertaining to financial accounts
- Medical information
- Information (such as names) associated with social media posts

2.4.1 GDPR and social media advertising with PSI

Under GDPR, should it be decided to collect visitors' data or track their behaviour for advertising, you must obtain the legal basis to do so. Explicit consent from visitors must be obtained.

- Visitors must be given a free and genuine choice to accept or reject (and be allowed to easily withdraw their consent)
- It must be stated what data will be collected and how it will be used
- The request for consent has to be in clear and plain language
- Inactivity doesn't constitute consent. Visitors must take an action (E.G. Pre-tick boxes for consent are not allowed)

3.0 Use of PSI social media accounts

The PSI social media accounts must only be used and created by authorised individuals for the purpose of meeting defined Society strategic objectives.

1. Furthering psychological science and its application
2. Promoting equal access to psychological knowledge, training and wellbeing
3. Always acting to the highest professional and ethical standards
4. Helping people, organisations and communities reach their full potential
5. Membership development, challenge and support

4.0 Goals and purposes of PSI social media accounts

As the social media landscape quickly changes and evolves, PSI members and volunteers are encouraged to think about new ways to use PSI social media accounts. However, account activity should not stray from the PSI goals of engaging and maintaining the Society's vision while becoming innovative with social media platforms which will help to build stronger relationships, increase Society prospects, and drive traffic to other digital properties.

4.1 Employees can typically meet these goals by:

- Distributing original content pieces such as blog posts, infographics and product photos
- Sharing third-party content pieces relevant to company target audiences
- Promoting special offers, including contests and discount events
- Interacting with the public which includes responding to them and prospect questions
- Monitoring the social web for brand mentions and responding accordingly

5.0 Approved users

Only approved users may access the PSI social media accounts.

Users will be approved by the PSI Data Controller – the Chief Executive Officer. The PSI Data Controller will consider approving users when an employee's, a member of a Division/Interest Group, or the Society's role involves creating and executing social media strategies or researching new and existing target audiences.

The Data Controller can revoke authorisation at any time.

5.1 Posting from the PSI's main social media accounts

The Communications & Branding Coordinator should be notified in so far as possible prior to any postings to the main PSI social media accounts as they monitor the account on behalf of the Data Controller (Chief Executive Officer). All posts should be sent to the Communications & Branding Coordinator for approval and formatting that is in keeping with PSI branding when possible. The Social Media Calendar takes precedence and it is important that notice is given to the Communications & Branding Coordinator should a post already be scheduled, and it needs to be removed/rescheduled.

If any post from Division/Special Interest Group is judged to present a reputational risk to the PSI, it will be requested that it is removed.

5.2 Division and Interest Group social media accounts

As a number of Divisions and Interest Groups manage their own social media accounts, it is vital that the Head of Communications is made aware of the Division/Interest Group member(s) who are charged with managing each account, as well as the usernames and passwords for such accounts.

Any change to the person responsible for the content of a Division/Interest Group social media account, or a change in username or password, should be immediately communicated to the PSI Communications & Branding Coordinator. This information will allow the Communications & Branding Coordinator to identify the contact person for a Division/Interest Group social media account should any problem arise with content, as well as being able to access a site should a username or password be forgotten or misplaced.

It is up to the Chair of each Division/Interest Group to ensure that this information (Appendix 1) is provided.

6.0 Creating social media accounts under the PSI Name

As the PSI must explore the advantages and disadvantages of expanding the Society's social media presence to new networks, the Chief Executive Officer must approve the creation of PSI social media accounts.

If employees see the opportunity to create a social media account that supports company goals, they should send their proposals to the Communications & Branding Coordinator.

6.1 Instant Messaging (IM) services

All messages composed and/or sent using PSI-provided electronic messaging resources i.e, WhatsApp messages, through Facebook Messenger and so on, must comply with PSI policies regarding acceptable communications.

PSI reserves the right to intercept, monitor, review and/or disclose any and all messages composed, sent or received.

All PSI business must be conducted through official PSI email and PSI Instant Messaging groups. This is due to GDPR and the communication of sensitive information.

7.0 Purpose of PSI social media accounts

The PSI's social media accounts may be used for many different purposes. In general, employees should only post updates, send messages or any other social media use when their objective is clearly in line with PSI strategic objectives.

For instance, employees may use PSI social media accounts to:

- Share **blog posts, articles and other content** created by the PSI
- Share **insightful articles, videos, media and other content** relevant to the business, but created by others
- Provide followers with **an insight into what goes on in the PSI**
- Support **new events** and other initiatives

Social media is a powerful tool that changes quickly. Employees are encouraged to think of new ways to use social media, making relevant proposals to the Communications & Branding Coordinator.

This Policy may be updated at any time without notice. Each time a user accesses a PSI social networking site, the most up to date version of the Policy will govern usage, effective upon posting. To remain in compliance, it is suggested that you review the Policy, as well as other PSI policies, at regular intervals. By continuing to post any content after such new terms are posted, you accept and agree to any and all such modifications to this Policy.

8.0 Safe, responsible social media use

The rules in this section apply to:

- Any employees using company social media accounts
- All Divisions and Interest Group using company social media accounts
- All members and volunteers of the Society using company social media accounts

8.1 Users must not:

- Create or transmit material that might be **defamatory or incur liability** for the PSI
- Post messages, status updates, and links to material or **content that is inappropriate**

  Note that inappropriate content includes pornography, racial or religious slurs, gender-specific comments, criminal actions or terrorism, or materials relating to cults, gambling and illegal drugs. This definition of inappropriate content or material

also covers any text, images or other media that could offend a person based on race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law

- Use social media for any **illegal or criminal activities**
- Send **offensive or harassing material** to others via social media
- Broadcast **unsolicited views** on social, political, religious or other non-business-related matters
- Send or post messages or material that **could damage the PSI's image or reputation**
- Discuss **colleagues, customers or suppliers** without their approval
- Post, upload, forward or link to **spam, junk email or chain emails and messages**

9.0 Copyright

The PSI respects and operates within copyright laws. Users may not use social media to:

- Publish or share any **copyrighted software, media or materials owned by third parties**, unless permitted by that third party. If staff wish to **share content published on another website**, they are free to do so if that website has obvious sharing buttons or functions on it
- Share links to **illegal copies** of music, films, games or other software

10.0 Security and data protection

10.1 Maintain confidentiality

Social media users must not:

- Share or link to any content or information owned by the PSI that could beconsidered **confidential or commercially sensitive**
- Share or link to any content or information owned by another company or person that could be considered **confidential or commercially sensitive**
- Share or link to data in any way that could breach the PSI's **data protection policy**

10.2 Protect social media accounts

- PSI social media accounts should be **protected by strong passwords** that are changed regularly and shared only with authorised users
- Wherever possible, employees should use **two-factor authentication** (often called mobile phone verification) to safeguard company accounts.

- PSI staff must not use a new piece of **software, app or service** with any of the PSI's social media accounts without receiving approval from the Data Controller/Head of Communications

10.3 Avoid social media scams

- PSI staff should be vigilant for **phishing attempts**, where scammers may attempt to use deception to obtain information relating to the PSI and/or Society members
    - Employees should never reveal sensitive details through social media channels. Member identities must always be verified in the usual way before any account information is shared or discussed
- Employees should **avoid clicking links** in posts, updates and direct messages that look suspicious. In particular, users should look out for URLs contained in generic or vague-sounding direct messages

11.0 Policy enforcement

11.1 Monitoring social media use

Company IT and Internet resources — including computers, smartphones and internet connections — are provided for legitimate business use. Therefore, the company reserves the right to monitor how social networks are used and accessed through these resources.

Any such examinations or monitoring will only be carried out by authorised PSI staff members.

Additionally, all data relating to social networks written, sent or received through the PSI computer systems is part of official PSI records.

The PSI can be legally compelled to show such information to law enforcement agencies or other parties.

11.2 Potential sanctions

Knowingly breaching the PSI Social Media Policy is a serious matter.

The persons actions will be investigated under the code of practice.

Breaches of this Policy will be investigated, and the Society retains the right to take necessary action.

For further information, contact communications@psychologicalsociety.ie

Appendix 1 – Letter of Undertaking

The Psychological Society of Ireland
Floor 2, Grantham House
Grantham Street
Dublin 8, D08 W8HD

T +353 1 472 0105
E membership@psychologicalsociety.ie
W www.psychologicalsociety.ie

Twitter Account information for Divisions and Special Interest Groups

Any change to the person responsible for the content of a Division/Special Interest Group social media account, or a change in username or password, should be immediately communicated to the PSI Communications & Branding Coordinator. This information will allow the Communications & Branding Coordinator to identify the contact person for a Division/Special Interest Group social media account should any problem arise with content, as well as being able to access a site should a username or password be forgotten or misplaced.

Designated User:

Users with Access:

Handle:

Email/Login:

Password:

Division/Special Interest Group:

Signed:

Date: