National Examining Board for Dental Nurses.

NEBDN

Controlled Document

Document Name:	**Social Media Policy**
Document Version Number	6
Agreed by Communications	21.06.2021
Agreed by CEO/Senior Management:	22.06.2021
Review Schedule	Biennial
Next review due	July 2023
Owner (Responsibility)	Jade Monori, Marketing Manager
Pass amendments to	Lindsay Price Head of Innovation & Strategy
Revision History	See appendix

Document description

Social media channels provide important and exciting opportunities for NEBDN and its constituent parts to communicate and engage with a wide range of audiences and stakeholders. These channels also provide a range of professional and personal opportunities for staff and Associates.

1. Introduction

This policy describes the governing use of social media at NEBDN and provides guidance to staff and Associates on how to safely and productively use social media to maximise the range of benefits it offers, whilst mitigating associated risks. In particular, it provides information on responsibilities when communicating via the charity's social media accounts; expectation of staff on individual personal and professional accounts, and expectations of Course Providers in relation to social media.

Staff should comply with sections 1 and 2 of the policy. Course Providers and Associates should comply with sections 1 and 3 of the policy.

1.1 Policy objectives

- To provide staff and Associates with information on NEBDN requirements and expectations regarding social media
- To ensure a consistent approach to social media across the charity
- To set out the legal risks associated with social media use
- To ensure staff and Associates do not compromise their personal security or the security of NEBDN
- To outline channels for escalation of issues or concerns

1.2 Policy scope

This policy applies to all staff and Associates (including volunteers) at NEBDN who use social media while working —whether it's for business or personal reasons.
It applies whether social media use takes place on charity premises, while travelling for business, or while working from home.
Social media sites and services include (but are not limited to):

- Popular social networks like **Twitter** and **Facebook.**
- Photographic social networks like **Flickr** and **Instagram.**
- Professional social networks like **LinkedIn.**

NEBDN's corporate accounts include:

- Twitter
- Facebook
- LinkedIn
- YouTube

1.3 Responsibilities

Everyone who operates a corporate/charity social media account or who uses their personal social media accounts at work, has some responsibility for implementing this policy. However, the **communications manager** has the key responsibilities:

- For ensuring that NEBDN, its staff, Associates and volunteers uses social media safely, appropriately and in line with the charity's objectives.
- For providing apps and tools to manage the charity's social media presence and track any key performance indicators. They are also responsible for proactively monitoring our social media security and distributing marketing ideas and campaigns through our social media channels.

The communications manager is responsible for ensuring requests for assistance and support made via social media are followed up.

1.4 Legal risks

There are a number of legislations relevant to the use of social media and these are listed in the appendix which cover items such as defamation, malicious content and property infringement.

2 Staff

2.1 Policy acceptance

This policy forms part of the NEBDN contractual requirements of staff members

2.2 Appropriate use

Staff may make reasonable and appropriate use of social media from NEBDN. Time spent on social media during working hours should not interfere with other duties.

2.3 Public Interest Disclosure (whistleblowing)

Any disclosure of serious malpractice, corruption, wrongdoing or impropriety should be made to either the communications manager or a member of the senior management team. Where an employee releases such information through social media, NEBDN's incident management form will be initiated before any further action is taken.

2.4 Social media account management

All social media accounts used professionally must adhere to the NEBDN's brand guidelines, and the account profile information should clearly state the purpose of the account and that views are your own.
It is important that all social media accounts are kept up to date, posted from regularly and monitored on a frequent basis. Questions regarding NEBDN should be responded to promptly within operating hours by the appropriate person.

2.5 Social media posts

All posts from corporate or professional social media accounts represent NEBDN. It is vital that messages posted are carefully considered, appropriate and do not damage the reputation of NEBDN or otherwise bring it into disrepute. Safeguards should be put in place to minimise the risk of communication errors via social media, including checking content with a colleague before publishing.

Posts must be in line with the values and ethics of NEBDN and all relevant NEBDN policies, including Regulations for the Use of IT Services. Those posting content on corporate social media accounts **must not**:

- Post or promote any content that would amount to a breach of the criminal law in the jurisdiction of the United Kingdom.
- Post or promote content which harasses, bullies or otherwise intimidates
- Post or promote content which instructs, causes or coerces others to harass, bully or otherwise intimidate
- Post or promote content intended to incite violence or hatred
- Post or promote abusive content relating to an individual's age, disability, gender reassignment, marriage/civil partnership, pregnancy/maternity, race, religion or belief, sex or sexual orientation.

Content posted or promoted on corporate accounts must be respectful of others and courteous. Corporate accounts must not be used to criticise or argue with colleagues, candidates, Associates or competitors.

When posting on an account, it is vital to have legal considerations in mind (see section 1.4). This includes, but is not limited to, ensuring that posts do not breach confidentiality, make defamatory comments or breach copyright. Communications through social media **must not:**

- Include confidential information about an individual or organisation
- Discuss NEBDN's internal workings or reveal future plans that have not been communicated to the public
- Use someone else's images or written content without permission and/or without acknowledgement

- Use, disseminate, publish or distribute any content, mark, design or any text; the use of which would amount to an infringement of Intellectual Property Rights of others.

It is also important that content is accurate and does not commit to something which NEBDN does not intend to deliver. If a mistake is made, it is important to be transparent and inform the communications manager to update the page with a correction.

2.6 Account security

Social media accounts are at risk of a cyber security breech for example hacking and this can cause significant reputational damage and potentially serious misinformation for stakeholders. There are also considerable resource implications following on from any breach in security such as a compromised social media account.
Please ensure you don't share the password for any corporate or personal social media accounts with anyone unless necessary. If logging into a corporate account, please locate from a shared file and not through use of email or other apps.

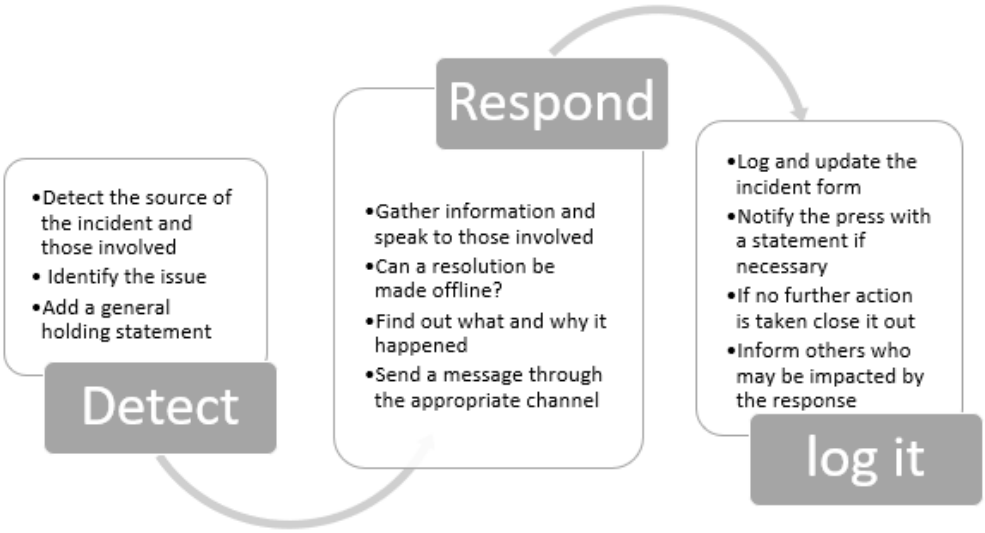
2.7 GDPR

Please ensure individual's personal data is not put at risk through the use of social media by anyone working for or with the organisation.

2.8 Escalating concerns and issues

If a social media account has been hacked or a post from a corporate account attracts a number of negative comments and it is not clear how best to respond, staff should flag this with the communications manager or their line manager.
If an individual is contacted for comments about the organisation for publication anywhere, including in any social media outlet, the enquiry must be directed to the communications manager.

2.9 Escalation process
NEBDN monitors comments and reviews on social media. Should an individual make an allegation or comment that is damaging to an individual or to the organisation, NEBDN will follow a three-step process. The incident will be logged, an investigation will be made, and further actions may be taken.



2.10 Social media in an emergency

We have stringent procedures set-up to ensure social media is monitored at all times, however, under extenuating circumstances social media may not be checked each day after hours. Should you need to contact someone in relation to an urgent media situation please email the below contacts.

- Head of Strategy & Innovation – Lindsay.price@nebdn.org
- Head of Quality and Standards – henry.payne@nebdn.org
- Marketing and Communications Manager – communications@nebdn.org

2.11 Photography

When using images for social media you must ensure you have the individual's permission for GDPR and copyright purposes. If you are taking an image on behalf of NEBDN please ensure you use a high-quality phone or camera to provide a clear quality photo – blurry or dark images are no good.

3. Course Providers and Associates

3.1 Policy Acceptance

Course Providers presence on social media is a public record which is interlinked with individual reputation. Social media can be a positive tool, but it is important to carefully consider post content and account security in order to mitigate the associated risks.

Posting offensive, inappropriate or unlawful material can have a number of serious consequences, including, but not limited to:

- Significantly impacting on a candidates academic and long-term employment prospects
- Damaging NEBDN's reputation
- Legal action
- Dismissal of affiliation with NEBDN

3.2 Course Provider logo use

NEBDN's logo and acronym is a registered trademark. Using our logo incorrectly or committing trademark infringement may result in further legal proceedings.

If you are a Course Provider, it is your responsibility to adhere to the above and ensure you include the course provider logo on any digital or printed marketing material or leaflets where the NEBDN name is used. The logo below is acceptable. Should you require a copy of our logo please email communications@nebdn.org

National Examining Board for Dental Nurses®
Accredited Course Provider

Individuals who breach any of the requirements set out above will be subject to disciplinary action in accordance with the organisation's disciplinary policies.

3.3 Social media posts

When posting on social media, Course Providers and Associates **are required to**:

- Conduct themselves in a manner which demonstrates respect for NEBDN staff, candidates and property, and for other members of the local community in general
- Use the handle @NEBDNoffice or hashtag #NEBDN in social media updates
- Act in line with the Course Provider agreement
- Ensure their posts do not raise any copyright or intellectual property issues or the other legal issues outlined in 1.4 above
- Must adhere to the course providers use of logo 3.2.

When posting on social media, Course Providers and Associates **must not**:

- Discuss examination services provided by NEBDN, if it relates to any topics that are not public information.
- Breach our Standards of Performance and Conduct
- Fraudulently assume the identity of another
- Post or promote content which harasses, bullies or otherwise intimidates.

3.4 Photography

If you are using an image that belongs to NEBDN, please ensure you have permission by NEBDN before posting due to copyright.

3.5 Escalation concerns and issues

Any disclosure of malpractice, wrongdoing or impropriety should be made to the communications manager via email or calling our office 01772 429 917 within 24 hours. **Please provide a screenshot image where applicable in case the content is not found at a later date.**

If an individual is contacted for comments about the organisation for publication anywhere, including in any social media outlet, the enquiry must be directed to the communications manager.

3.6 Escalation process

See 2.9 for process of escalation.

3.7 Who to contact in an out of hours emergency?

Please see 2.10 social media in an emergency

PLEASE SEE APPENDIX BELOW

Appendix

Legal risks supporting documents

- Defamation: posting reputation, which has caused, or is likely to cause, harm
- Malicious falsehood: posting untrue and damaging content with an improper motive, resulting in financial loss for the subject
- Harassment: subjecting someone to a course of conduct that causes them distress or alarm, including stalking, trolling and cyber-bullying
- Intellectual property infringement: posting content which copies a substantial part of a work protected by copyright
- Malicious Communications Act 1988: prevents conveying a threat, a grossly offensive or indecent message or false information with the intention to cause distress or anxiety to the reader or recipient
- Section 127, Communications Act 2003: prevents the use of public electronic communications equipment to send a message that is false, grossly offensive, or of an indecent, obscene or menacing character, whether received by the intended recipient or not
- Computer Misuse Act 1990: prevents the unauthorised access, modification and use of computer material or the use of a computer to assist in a criminal offence, including accessing confidential information and thereby impersonating another person through social media.

Information reproduced from Thomson Reuters, Practical Law.

Legislation for reference:

- Course Provider Agreement 2020
- Communications Act 2003
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Counter Terrorism and Security Act 2015 (Prevent)
- Criminal Justice and Immigration Act 2008
- Data Protection Act 1998
- Data Retention Investigatory Powers Act 2014
- Defamation Act 2013
- Education (No. 2) Act 1986 (Freedom of Speech)
- Education Act 1986; Education Reform Act 1988 (Academic Freedom)
- Employment Rights Act 1996
- Equality Act 2010
- Freedom of Information Act 2000
- Freedom of Information (Scotland) Act 2002
- Human Rights Act 1998
- Malicious Communications Act 1988
- Obscene Publications Act 1959 and 1964
- Police and Criminal Evidence Act 1984
- Police and Justice Act 2006
- Prevention of Terrorism Act 2005
- Protection from Harassment Act 1997
- Public Order Act 1986 (as amended by the Racial and Religious Hatred Act 2007

Revision History of Social Media Policy

21 June 2021
30 July 2020
8 July 2020
28 October 2019
24 July 2019
24 May 2018