**PCIG Consulting Template**

**Social Media Staff Policy**

**Version: 2.0**

**Date: 1 April 2021**

**This template is for use by Practices to Comply with the GDPR requirement to have a policy regarding processing of patient data. The template is Generic in design as PCIG Consulting have clients across the UK, local sharing arrangements and area specific sharing or processing will need to be added by the practice.**

**Change Control**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **To** | **Change** | **Date** |
| **1** |  |  |  |
| **1** | **2** | **Reviewed and updated** | **1 April 2021** |

[Practice Name]

**Social Media Staff Policy**

**Document History**

|  |  |
| --- | --- |
| Document Reference: | … |
| Document Purpose: | This policy sets out the practice [practice name] expect from all staff, including those working on behalf of the Practice, when a using social media |
| Date Approved: | 1 April 2021 |
| Version Number: | 2 |
| Status: | FINAL |
| Next Revision Due: | 1 April 2022 |
| Developed by: | Paul Couldrey – IG Consultant |
| Policy Sponsor: | Practice Manager |
| Target Audience: | This policy applies to any person directly employed, contracted, working on behalf of the Practice or volunteering with the Practice. |
| Associated Documents: | All Information Governance Policies and the Information Governance Toolkit, and Data Security and Protections Toolkit 2021 |
| DS&P Toolkit Standard |  |

This document sets out the [Practice Name] policy on personal use of social media. This policy applies to what is written/posted/streamed on social media sites by staff in a personal capacity which relates to their work.

[PRACTICE NAME] recognises that many employees participate in social networking sites outside of work hours. In the majority of cases this is uncomplicated and trouble-free. The intention of this policy is not to interfere with an employee’s personal life however there are potential risks/nuisances associated with the use of social media; risks which individuals may not even be aware of. An erosion of the boundary between work-life and home-life can sometimes have a negative impact on the relationship between an individual and their employer. Therefore, there is a need to provide individuals with clear guidelines on what is and what is not considered to be appropriate personal use of social media, safeguarding the reputations of individuals and the organisation.

The main principle behind this policy is that conduct on-line should be judged against the same high standards of behaviour which [PRACTICE NAME] expects of its employees. Employees should think carefully about what they post on the internet and be aware that individual privacy settings are not always sufficient to stop others seeing your content/distributing your content. Social media sites frequently alter their terms of usage

# Definition of Social Media

The term ‘social media’ is used to describe on-line technologies and practices that are used to share information, knowledge, and opinions. Social media services and tools can involve a combination of technology, telecommunications and some form of online social interaction and can use a variety of different formats, e.g., text, images, video and audio.

Social media as a term includes social networking (e.g., Facebook, TikTok, Bebo and Linkedin), blogging applications (e.g., Twitter, LinkedIN, WordPress), multimedia sharing and networking applications (e.g. YouTube, Flickr and Skype), information sharing sites (e.g. Wikipedia), review and opinion sites (e.g. Google Answers and Yahoo! Answers), forums (e.g. Mumsnet, Digital Spy and iVillage), dating sites and personal web pages. This list is not exhaustive.

This policy is equally applicable to the use of social media via mobile access e.g., Smartphones and tablets includes use of applications (apps)

# SCOPE

This policy applies to all employees of [PRACTICE NAME], whether full time or parttime, whether on permanent contracts, fixed term or bank (as and when required) contracts. The policy also applies to [PRACTICE NAME] official volunteers including volunteers and staff from commissioned services.

This policy applies to all contractors, partnership organisations and those who have access to the internet via the [PRACTICE NAME] infrastructure

This policy relates to the personal use of social media whether during work hours or outside of work and where there is a significant connection with the employee’s work reputation, the Practice’s reputation and where colleagues are referred to.

# Employee responsibilities when at work

All [PRACTICE NAME] IT systems and services are provided as business tools. Employees who have authorised access to the internet at work for business use only.

As a rule, [PRACTICE NAME] employees are not allowed access to social media sites such as Facebook and Twitter on the [PRACTICE NAME] network unless authorised for business purposes by the Practice Manager or delegated member of staff.

Where employees bring their own personal mobile devices into the workplace, they must limit their use of these devices in relation to personal use of social media to official rest breaks, such as lunchtimes.

# Employee responsibilities when not at work

All employees are responsible for any information they make available on-line whether this was posted during work hours, during breaks or when not at work. The practice considers employees to be responsible and accountable for information contained on their social networking page or blog.

Employees need to be aware of what is posted/uploaded to sites they control and that they would be expected to manage any inappropriate material responsibly.

[PRACTICE NAME] reserves the right to contact the social media provider and request removal of materials in serious cases involving risk of reputational damage to the Practice as the employer.

Employees therefore must ensure that when engaging in social media activity they abide by the following standards: Employees must not:

* Send information, forward e-mails, or send images (e.g., photos, cartoons, graphics) on-line about [PRACTICE NAME], its services, facilities, staff, patients or third parties, which are confidential, defamatory, discriminatory, harassing, illegal, threatening, intimidating or which may incite hatred (e.g., sectarianism/racism/homophobia).
* Direct defamatory, threatening, or intimidating comments on-line towards other [PRACTICE NAME] employees. If they do so, this will be judged in terms of the amount of harm caused and the size of the audience who will see the comments (e.g., how many people would see the comments on-line and just how bad were those comments considered to be?).
* Send or post images/photos of patients, services users, or employees in the workplace, that would not otherwise be considered to be a public place, unless the express authority of the subject has been secured and that consent is based upon a full understanding of how the image will be used.
* Employees will inevitably discuss aspects of their working day with others, either face-to-face, over the telephone or on-line. Employees must however be cautious about discussing work-related issues and complaints in a manner which could cause reputational damage to individuals, their own reputation or that of the Practice as their employer. Legitimate concerns should always be addressed through the appropriate Practice policies
* Use their works e-mail address to register on a social network or e-commerce website (e.g., eBay, Amazon, Groupon).

# Employees are advised:

* That if they disclose the name of the Practice as their employer, they should make it clear when publishing their opinions on-line, that these are their own personal views and that they do not represent the views of [PRACTICE NAME].
* Consider the principles of the Staff code of confidentiality and the Practice Data Protection Policy. Any breaches of this policy may be subject to the Practice’s Disciplinary Policy and other associated policies

# Approval

These procedures have been approved by the undersigned, and they will be reviewed on an annual basis and in particular in the event of an incident as part of the lessons learned process.

# Training

[PRACTICE NAME] must ensure that all staff undertake appropriate records management training on information governance issues soon after joining the practice and that existing staff receive periodic update training. Staff who have responsibility for records management should undertake records management training on an annual basis.

# Equality and Diversity

The Practice aims to design and implement policy documents that meet the diverse needs of the services, population and workforce, ensuring that none are placed at a disadvantage over others. It considers current UK legislative requirements, including the Equality Act 2010 and the Human Rights Act 1998, and promotes equal opportunities for all.

This document has been designed to ensure that no-one receives less favourable treatment due to their personal circumstances, i.e., the protected characteristics of their age, disability, sex (gender), gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy and maternity. Appropriate consideration has also been given to gender identity, socio-economic status, immigration status and the principles of the Human Rights Act.

In carrying out its functions, the Practice must have due regard to the Public-Sector Equality Duty (PSED). This applies to all the activities for which the Practice is responsible, including policy development, review and implementation.

# Due Regard

This policy has been reviewed in relation to having due regard to the Public-Sector Equality Duty (PSED) of the Equality Act 2010 to eliminate discrimination, harassment, victimisation; to advance equality of opportunity; and foster good relations.

# Review and Monitoring

The Practice Manager is responsible for regular monitoring of the quality of records and documentation and managers should periodically undertake quality control checks to ensure that the standards as detailed in this policy are maintained.

This policy will be reviewed every two years unless new legislation, codes of practice or national standards are introduced.