**Social Media Policy Template**

**Please use this template and adapt to the needs of your organisation**

**Approved on:**

**Next Review Date:**

**Introduction**

The Organisation is committed to ensuring that all its staff are aware of how social media should be used in, and outside of, the workplace. This includes use in both a professional or personal capacity. The Organisation recognises the impact that social media could have on the reputation or image of an organisation or associated persons, therefore appropriate usage is vital.

Employees should be aware that the field of technology and digital media is constantly changing and developing, therefore this policy should be followed as closely as possible where relevant.

**Scope**

This policy applies to all employees of the organisation.

**Principles**

The main aims of this policy are to:

* Ensure that employees are aware of what is meant by social media and use of social media;
* Equip employees with clear guidelines about how social media should be used:
* in the workplace itself;
* in a professional capacity; and
* in a personal capacity.
* Outline what is understood to be appropriate and inappropriate behaviours on social media in relation to The Organisation and associated bodies and persons;
* Advise employees on safety and security when using social media;
* Explain the procedure for reporting inappropriate behaviour on social media;
* Outline the consequences of improper use of social media in connection to The Organisation and how this would be dealt with; and
* Advise employees on whom to contact for further information and guidance about using social media, online safety, organisational branding, and any other queries.

**Definition of social media**

For the purposes of this policy, social media is defined as all forms of electronic communication through which users can share data and information with each other and in a public forum.

Forms of electronic communication may include online platforms, websites, computer software and apps. Shared data includes, but is not limited to, words, images, podcasts, audio files and video content.

Popular examples of social media include Facebook, Twitter, Instagram, Youtube, Snapchat, Whatsapp, Tumblr, LinkedIn, Pinterest, Vimeo, TikTok and blogging platforms.

**The use of social media in the workplace**

With the rise of internet connectivity and smartphones, many employees have access to social media in the workplace both on workplace equipment, and personal communication devices. The reasonable use of social media in the workplace or during normal working hours is permitted, as long as this does not interfere with an individual’s duties or disturb others. However, excessive or inappropriate use could result in disciplinary action.

Commenting in real-time on social media at work, for example live-tweeting during a meeting, is not appropriate.

The Organisation reserves the right to investigate an employee’s use of social media if the employee is under investigation for breach of this policy, or any other diocesan policy.

**The use of social media in a professional capacity**

The Organisation encourages employees to make reasonable and appropriate use of social media as part of their work, depending on the role. Social media is an important part of how diocesan staff interact with other members of staff and clergy, parishioners, and the general public. It can be a useful tool in certain teams, for example in order to promote events and initiatives. Depending on an employee’s role, a diocesan account may be used for such purposes.

Employees must be aware at all times that, while contributing to diocesan social media activities, they are representing the organisation.

Employees should use the same safeguards as they would with any other form of communication about the organisation in the public sphere. These safeguards include:

* making sure that the communication has a purpose and a benefit for the organisation;
* obtaining permission from a manager before embarking on a public campaign using social media; and
* getting a colleague to check the content before it is published.

**The use of social media in a personal capacity**

Many employees use social media in a personal capacity at home and outside their working hours. Although they are not acting on behalf of the organisation, employees must be aware that they can damage the reputation of The Organisation if they are recognised as being a diocesan employee.

It is better for employees not to associate themselves with work online where possible.

**Online behaviour on social media**

Any communications that employees make in a professional or personal capacity through social media must not:

* bring The Organisation into disrepute, for example by:
* criticising or arguing with colleagues, members of the public;
* making defamatory comments about individuals or other organisations or groups; or
* posting images that are inappropriate or links to inappropriate content;
* do anything that could be considered discriminatory against, or bullying or harassment of, any individual for example by:
* making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief, or age;
* using social media to bully another individual (such as a diocesan employee); or
* posting images that are discriminatory or offensive (or links to such content);
* breach confidentiality, for example by:
* revealing information owned by The Organisation;
* giving away confidential information about an individual (such as a colleague or parishioner) or organisation; or
* discussing the Diocese's internal workings or The Organisation’s future business plans that have not been communicated to the public;
* breach copyright, for example by:
* using someone else's images or written content without permission; or
* failing to give acknowledgement where permission has been given to reproduce something.

All of the above could be classed as either misconduct or gross misconduct depending on the nature of the allegation and may be dealt with through the use of the Disciplinary Policy.

**Online safety and security**

It is essential to consider the following cyber security guidelines when using social media or other online platforms in the workplace:

* At the end of an online session, an employee must always be sure to log out of any social media accounts accessed on workplace or communal equipment, and not allow browsers or other software to remember passwords. Computer monitors should not be left unattended if unlocked;
* Passwords for diocesan laptops and any online accounts should be changed on a regular basis, or when prompted. Passwords must not be shared with any other person (with the exception that a team or teams may use a shared account for particular online tools);
* Employees should consider the privacy settings on their social media accounts which might affect whether colleagues or members of the public can see particular aspects of their social media profile;
* When in doubt, an individual should not share or publish personal data or information which could link back to them or their place of work; and
* If an employee suspects that a social media account has been hacked, if they receive unwanted messages, or if a phone or laptop are stolen, they should notify the person in charge of Information Technology, Manager, immediately.

**Reporting inappropriate behaviour on social media**

If any individual becomes aware of an employee’s misuse of social media, this should be reported immediately to their Manager/Management committee who will then take further action if necessary.

**Disciplinary action over social media use**

Employees should note that any breaches of this policy may lead to disciplinary action. Serious breaches, for example incidents of bullying of colleagues or social media activity that might cause serious damage to the organisation, may constitute gross misconduct and lead to summary dismissal and the employee may be legally liable for any reputational damage.