AUSTRALIAN COBBERDOG SOCIETY

Social Media Policy

Date	12th June, 2024 (Ratified 9th August, 2024)
Purpose	The Australian Cobberdog Society (ACS, or hereon referred to as 'the Society') Social Media Policy outlines protocols for using social media to undertake official business, and provides guidance for Society members in their personal use of social media.
Applicable to	This policy applies to all Society members, inclusive of founding members, breeder members and owner/enthusiasts. The Society is committed to ensuring all members understand the Social Media Policy and expectations when making public comment both in their professional and personal lives.
Policy	The Social Media Policy outlines protocols for using social media to undertake official Society business, and provides guidance for owners in their personal use of social media or making public comment online. The policy provides advice on how to use social media, both in the course of official ACS duties, and as a private citizen. It has been developed to assist all stakeholders to be mindful of their obligations and responsibilities as members of the ACS. The Social Media Policy applies to all committee members and is strongly advisable that all owners uphold these same expectations to avoid consequence.

Usage	The same high standards of conduct and behaviour generally expected of community members also apply when participating online through social media. Online participation should reflect and uphold the values, integrity and reputation of the Society, in alignment with the Constitution.

1 Personal use of social media and making public comment online

1.1

Australian Cobberdog Society members have the same right to freedom of expression as other members of the community, subject to a legitimate public interest in maintaining impartiality towards the Society.

1.2

Interactions online should mirror the professionalism expected in person. Respect others' opinions and act courteously, avoiding discrimination, defamation, bullying, or harassment.

1.3

The Society respects the right of members to participate in political, advocacy, and community activities. In doing so, however, members must behave in a way that does not seriously call into question their capacity to act impartially. It is also important that the reputation of the Society is not placed at risk by comments that members make. Members should be aware that content published online and on social media is, or may become publicly available, even from personal social media accounts. It is expected that members take reasonable steps to ensure that any social media use or public comments made about the Society, fall within the following parameters:

Members must ensure they:

- Do not use an ACS email address to register personal social media accounts
- Do not make comments that are unlawful, obscene, defamatory, threatening, harassing, discriminatory or hateful to, or about ACS members
- Do not make comments that are, or could be perceived to be made on behalf of the Society, rather than an expression of a personal view
- Must not compromise their capacity to fulfil duties as an ACS member in an impartial and unbiased manner.

- Must make clear that any views expressed are their own, and not those of the Society.

1.4

When considering making personal comments, Society members should reflect on the following questions:

- Could your comments cause the Society or other stakeholders to lose confidence in your ability to work in an impartial and professional manner?
- Are your comments consistent with how the community expects the Society to operate and behave?
- Could your comments lower or undermine the reputation of the Society?
- Are your comments lawful? For example, do they comply with anti-discrimination legislation and laws relating to defamation?
- Would you be comfortable if your manager read your comments?
- What if someone takes a screenshot of your comments and then circulates these around?I

1.5 Personnel with access to the Society's website and social media accounts are limited to the president and secretary for a minimum of two years from the establishment of the Society. Should this role be delegated to another financial member, it will be voted and agreed upon in a committee meeting. Passwords for Social Media will be changed:

(a) if the security of the social media or website has been compromised
(b) if there is reason to believe that the social media has been infiltrated by a third party
(c) when a new president and secretary commence

2 **Content published on the internet**

Content can be easily replicated and shared beyond the original intended audience who may view it out of context or use it for an unintended purpose. For example, private messages or posts can be saved, screenshot, and made public – with little potential for recourse. It is important to be aware that according to the terms and conditions of some third-party sites, the content published is the property of the site where it is posted and may be re-used in ways that were not intended. Before posting to a social media site it is important for users to understand the tool/platform, read the terms of service and user guides, and look through existing content to get an idea of the

posting etiquette and any cultural and behavioural rules or protocols associated with that social media platform. Do not rely on a social media site's default or adjustable security settings as any guarantee of privacy.

3 **Record Keeping**

All ACS members have an obligation to ensure that key decisions and events are recorded in a way that captures the important features of a discussion or decision, presents a faithful and accurate account and can be easily retrieved when needed. Social media platforms are often provided by third-party providers and are not official record keeping systems.

Personal information about individuals cannot be provided to third-parties without their consent. The email address of ACS members or stakeholders and other identifiable information must be treated with discretion and care.

A failure to comply with this Policy may constitute a breach of the ACS Code of Conduct. Examples of failure to adhere to the Code of Conduct in a social media setting include, but are not limited to:

- making derogatory or obscene posts about a member on a social networking site
- criticising the ACS, its policies or individuals in a way that brings the Society into disrepute
- posting derogatory comments or images about Society members from a personal account
- disclosing non-publicly available information about income payments in a blog post.

A suspected breach of the ACS Code and this policy will instigate an investigation by the Society, that may result in:

- termination of membership
- suspension
- reprimand
- legal action.

Security Breach

The following data breach response plan (response plan) sets out procedures and clear lines of authority for the Society in the event it experiences a data breach (or suspects that a data breach has occurred).

There is no single method of responding to a data breach. Data breaches must be dealt with on a case-by-case basis, by undertaking an assessment of the risks involved, and using that risk assessment to decide the appropriate course of action. Depending on the nature of the breach, the response team may need to include additional staff or external experts, for example an IT specialist/data forensics expert or a human resources adviser. The Society's Response Team will comprise of the president, the secretary and the treasurer.

Step 1: Identify the breach

A suspected data breach may be discovered by a Society member or may be otherwise alerted by a member of the public or the media.

If the Society becomes aware of, or is notified of a data breach, the president will immediately notify the Response Team of the suspected data breach.

The Response Team will record the following:

- the time and date the suspected breach was discovered,
- the type of personal information involved
- the cause and extent of the breach, and
- the context of the affected information and the breach.

Step 2: Contain the breach

The Response Team should seek to understand, assess and contain the breach. As soon the Response Team is made aware of the breach or suspected breach, the Team should seek all the facts to enable an initial assessment of whether a data breach has or may have occurred and the seriousness of the data breach or suspected data breach. This should be done within the first hour of being so made aware.

The Response Team should co-ordinate any immediate action required to contain the breach. Depending on the breach, this may include contacting incorrect recipients requesting them to delete the email or requesting information be removed from a website.

Step 3: Notify

The Response Team must alert any affected stakeholders as soon as reasonably practicable after co-ordinating any immediate action. Notification must occur however within the same working day as being made aware of the breach and co-ordinating immediate action. Stakeholders should be informed of:

- a description of the breach or suspected breach,
- the action taken by the Response Team to address the breach or suspected breach,
- the outcome of that action,
- a view as to the seriousness of the breach, and
- a view as to whether any further action is required.

Notification can be an important mitigation strategy that has the potential to benefit both the entity and the individuals affected by a data breach. The challenge is to determine when notification is appropriate. Sometimes, notifying individuals can cause undue stress or harm. For example, notifying individuals about a data breach that poses very little or no risk of harm can cause unnecessary anxiety. It can also de-sensitise individuals so that they don't take a notification seriously, even when there is a real risk of serious harm. Each incident needs to be considered on a case-by-case basis to determine whether breach notification is required.

Step 4: Review

Once steps 1 to 3 have been completed, the Society will review and learn from the data breach incident to improve its personal information handling practices.

This might involve:

- a security review including a root cause analysis of the data breach
- a prevention plan to prevent similar incidents in future

- audits to ensure the prevention plan is implemented
- a review of policies and procedures and changes to reflect the lessons learned from the review
- changes to employee selection and training practices
- a review of service delivery partners that were involved in the breach

When responding to a data breach officers will undertake steps 1, 2 and 3 either simultaneously or in quick succession. At all times, the Society will consider what remedial action can be taken to reduce any potential harm to individuals.

4 Authorisation

Any official content uploaded onto social media platforms will be managed by the ACS delegate. This may be either the President or Secretary or another member as elected by the ACS committee.

4.1 Logo

No person, entity or organisation may use the Society logo without the direct express written permission from the Australian Cobberdog Society Inc.

The Copyright Act 1968 (Cth) regulates copyright in relation to original artistic works which includes logos. Section 36 states that a copyright infringement occurs when another person plagiarises a work commercially, without the owner's permission. Therefore, using another's company logo on your website could amount to a copyright infringement because it signifies an attempt to reproduce their artistic work.
(https://openlegal.com.au/can-i-use-a-companys-logo-on-my-website/)

The ACS Logo can be used by members with current membership status for the financial year in question. It can be displayed on:

1. Websites

2. Social Media

3. Email signatures

All Society members must respect the intellectual property rights of the organisation and other parties, making sure they don't infringe any intellectual property and expose the Society to expensive legal proceedings, and damages.

Society members may only post images and photographs if:

- they rightfully own the photograph
- they bred the dog that appears in the photograph
- they own the dog in the photograph
- they are a financial member of the Society
- they have written consent from the owner or breeder to publish the photograph and cite said owner or breeder.

Breach of intellectual property policy will result in action in accordance with the Constitution.