

## **Social Media Policy**

**Updated: Sept 2020**

**Due for Review: Sept 2021**

*We recognise that the internet provides unique opportunities to participate in interactive discussions and share information on particular topics using a wide variety of social media platforms including Facebook, Twitter, Instagram and What's App (not exhaustive). However, employees' use of social media can pose risks to our confidential and proprietary information, and reputation, and can jeopardise our compliance with legal obligations. To minimise these risks, to avoid loss and productivity and to ensure that our IT resources and communication systems are used only for appropriate business purposes, we expect employees to adhere to this policy.*

*This policy does not form part of employee's contract of employment and may be amended at any time.*

### **Who is covered by the policy?**

This policy covers all individuals working at all levels and grades, including trustees, senior managers, directors, employees, consultants, contractors, trainees, homeworkers, part-time and fixed-term employees, casual and agency staff, freelancers and volunteers (collectively referred to as staff in this policy).

### **Scope and purpose of the policy**

This policy deals with the use of all social media and online platforms.

It applies to the use of social media for both business and personal purposes, whether during office hours or otherwise. The policy applies regardless of whether the social media is accessed using our IT facilities and equipment or equipment belonging to members of staff.

Breach of this policy may result in disciplinary action up to and including dismissal.

Disciplinary action may be taken regardless of whether the breach is committed during office working hours, and regardless of whether our equipment or facilities are used for the purpose of committing the breach. Any members of staff suspected of committing a breach of this policy will be required to co-operate with our investigation, which may involve handing over relevant passwords and login details.

Staff may be required to remove internet postings which are deemed to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

## Personnel responsible for implementing the policy

Social Media content across all Rural Media platforms is the responsibility of, and managed by, the Social Media and Marketing Manager, Elle Adams. Project specific social media content creation may be delegated to specific project staff.

All managers have a specific responsibility for operating within the boundaries of this policy, ensuring that all staff understand the standards of behaviour expected of them and taking action when behaviour falls below its requirements.

All staff are responsible for the success of this policy and should ensure that they take the time to read and understand it. Any misuse of social media should be reported to our Social Media and Marketing Manager. Questions regarding the content or application of this policy should be directed to our Operations and Project Manager.

## Compliance with related policies and agreements

Social media should never be used in a way that breaches any of our other policies. If an internet post would breach any of our policies in another forum, it will also breach them in an online forum. For example, employees are prohibited from using social media to:

- take any steps that would damage the reputation of the charity or which may bring the charity in to disrepute;
- defame or disparage the charity or its affiliates, customers, clients, business partners, suppliers, vendors or other stakeholders;
- harass or bully other staff in any way or breach our anti-bullying and harassment policy;
- unlawfully discriminate against other staff or third parties or breach our equal opportunities policy;
- breach our data protection policy (for example, never disclose personal information about a colleague online);
- breach any other laws or ethical standards (for example, never use social media in a false or misleading way, such as by claiming to be someone other than you or by making misleading statements).
- Staff should never provide references for other individuals on social or professional networking sites, as such references, positive and negative, can be attributed to the charity and create legal liability for both the author of the reference and the charity

Employees who breach any of the above policies will be subject to disciplinary action up to and including termination of employment.

### **Personal use of social media**

We recognise that employees may desire to use social media for personal activities at the office or by means of our computers, networks and other IT resources and communications systems. We authorise such occasional use during rest breaks so long as it does not involve unprofessional or inappropriate content and does not interfere with your employment responsibilities or productivity. While using social media at work, circulating chain letters or other spam is never permitted. Circulating or posting commercial, personal, religious or political solicitations, or promotion of outside organisations unrelated to the charity's business are prohibited. Usage will be monitored and excessive or inappropriate use will result in disciplinary action.

### **Responsible use of social media**

The following sections of the policy provide staff with common sense guidelines and recommendations for using social media responsibly and safely.

Protecting our business reputation:

Staff must not post disparaging or defamatory statements about:

- a) our charity;
- b) our clients;
- c) our participants & contributors;
- d) suppliers and vendors; and
- e) other affiliates, funders and stakeholders, but staff should also avoid social media communications that might be misconstrued in a way that could damage our business reputation even indirectly.

With the exception of those in specifically appointed posts, staff should make it clear in social media postings that they are speaking on their own behalf. Write in the first person when communicating via social media.

Staff are personally responsible for what they communicate in social media.

Remember that what you publish might be available to be read by the masses (including the charity itself, future employers and social acquaintances) for a long time. Keep this in mind before you post content.

If you disclose your affiliation as an employee of our charity, you must also state that your views do not represent those of your employer. For example, you could state, "the views in this posting do not necessarily represent the views of Rural Media". You should also ensure that your profile and any content you post are consistent with the professional image you present to clients and colleagues.

Avoid posting comments about sensitive work-related topics, such as our performance. Even if you make it clear that your views on such topics do not represent those of the charity; your comments could still damage our reputation.

If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from making the communication until you discuss it with your line manager

If you see content in social media that disparages or reflects poorly on our charity or on our stakeholders, you should contact your line manager or XXXXXXXXXXX. All staff are responsible for protecting our business reputation.

### **Respecting colleagues, clients, participants, partners and suppliers:**

- Do not post anything that your colleagues or our customers, volunteers, business partners, suppliers, vendors or other stakeholders would find offensive, including discriminatory comments, insults or obscenity.
- Do not post anything related to your colleagues or our customers, volunteers, business partners, suppliers, vendors or other stakeholders that does comply with Rural Media's editorial policy.

### **Monitoring**

The contents of our IT resources and communications systems are our property. Therefore, staff should have no expectation of privacy in any message, files, data, document, telephone conversation, social media post conversation or message, or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on our electronic information and communications systems.

We reserve the right to monitor, intercept and review without further notice, staff activities using out IT resources and communications systems. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the systems as well as keystroke capturing and other network monitoring technologies.

We may store copies of such data or communications for a period of time after they are created, and may delete such copies from time to time without notice.

Staff should not use the organisations IT resources and communication systems for any matter that you wish to be kept private or confidential from the charity.