Charity Number: 1160538
Policy Documentation

SOCIAL MEDIA AND INTERNET POLICY

Policy Reference	02
Status	Approved
Original Author	Caroline Davies-Khan
Date Written	10th October 2016
Date Approved on	12th November 2018 (committee meeting)

1 Introduction

Our goals in making use of online communication tools including social media, or social networking sites are to

- Support our objective of increasing opportunities for people in our local area.
- Promote activities and events, primarily at the community centre
- Expand and strengthen our links with our local community and other organisations
- Better communicate with members of our community and target audiences

In addition to social media the Organisation needs to protect its data from attacks that could be sourced through the internet. This policy addresses the steps required to minimise to this threat.

2 Definitions

Term	Definition
Centre	The social hall managed by the Committee: Eastcott Community Centre, Savernake Street, Swindon, SN1 3LZ Telephone: 07599256969, e-mail: eastcottcommunity@yahoo.co.uk
Committee	The trustees who manage and run the **Centre**
Organisation	Eastcott Community Organisation
Phishing	the fraudulent practice of sending emails pretending to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.
Social Media	websites and applications that enable users to create and share content or to participate in social networking.
Social Media site	An individual internet site used for social media. e.g. Facebook, Twitter, Instagram, LinkedIn, Google+ and YouTube
Spam	irrelevant or unsolicited messages sent over the Internet, typically to a large number of users, for the purposes of advertising, phishing, spreading malware, etc. a tinned meat product made mainly from ham.

3 Why the policy exists

The Organisation recognises that social media can be a very helpful way to disseminate information and will use this where appropriate to share information and promote activities. The Organisation feels the need for this policy to broadly define how they will use the media for the best use of them and how they protect data against threats made via the internet.

4 Scope

Covers all social media interactions made on behalf of the Organisation by:

- Employees
- Trustees
- Volunteers

5 Responsibilities

Role	Responsibility
Events Co-ordinator	Oversee management of social media sites. Ensure minimum of 2 administrators per site. Nominate which sites we have a presence on.
Administrators	To administer social media site in line with policy

6 Policy

6.1 The Organisation;

- will follow the constitution, charitable objectives and policies (especially Confidentiality) in all social media interactions.
- will ensure that once they establish a presence in a social media site, it will be updated regularly according to the conventions of the site.
- will ensure that where there is a social media presence, there are a minimum of two nominated volunteers to update content and respond to questions.
- will encourage training in the use of social media for their team where needed and appropriate. This may be sourced from other organisations.
- will aim for consistency of messages and actions across all social media sites.
- will identify themselves clearly in what they write and what they post. When acting on behalf of the organisation, this should be made clear.
- will adhere to copyright rules. They will properly cite their sources and seek clarification of copyright.
- may share articles, and information that has relevance to the community and meets their objectives. Consideration will be given to the impact of doing so.
- will choose which social media sites to use.
- will ensure secure passwords are used and known by the Chair, Vice Chair and Events Co-ordinator as well as those administering the site.
- will endeavour to get their facts straight before posting them on a social media site.
- will understand the content contributed to a social media site could encourage comments or discussion of opposing ideas.
- will be aware that a presence in the social media world is or easily can be made available to the public at large.
- will treat positive posts as feedback and acknowledge them as such.

- will send messages containing personal/contact information using email not messaging by social media private messaging.
- will delete social media private messages from our inbox at least every 6 months.

6.2 Trustees, employees and volunteers

- will not use their identity to represent the organisation outside the scope of its mission and objectives.
- will be responsible for what they write and what they post.
- use good judgment and exercise caution when posting, ensuring it does not reflect badly on the Organisation.
- can post on behalf of the organisation using their personal social media accounts but must make it clear that they are representing the organisation. For example, a suggested response when advertising the hall as a venue on a social media post is *'Hello, I am a member of Eastcott Community Organisation. We are a group of volunteer residents that manage a community facility and may have a space available. Please contact us at …..'*
- must use their own discretion on how they use their personal social media accounts in relation to the organisation. They are not expected to use it to further their work with the organisation unless they wish to do so. Certain functions of social media are outside the control of the organisation (eg "tagging" by those outside the organisation) and it is the responsibility of the individual to use privacy settings if they do not wish this to happen.
- will understand that airing personal grievances relating to the organisation on their personal social media sites will be dealt with under the disciplinary and grievances policy

6.3 Dealing with negative posts

The Organisation

- shall not engage in arguments or "flame wars," but in civil discourse.
- will moderate all comments and responses to their posts. They will ensure that no spam, profanity, defamatory, inappropriate or libellous language will be posted to their sites. Neither will they use such language when they post comments to other people's sites. In the case of persistent, extreme or potentially illegal comments, the Organisation has the right to block or ban a user from their page or site, and report to the police or take legal action as in accordance with their behaviour policy.
- where possible, action would be discussed by the committee but in certain circumstances, administrators would need to take immediate action. Users of the sites should also be aware that individual volunteers may also take action if comments on a public site are directed at them.
- will use a standard response to any offensive message posted to the site, an example response could be:
  ''I am writing to you in my capacity as (position) of Eastcott Community Organisation and one of the managers of the Eastcott Community Centre Facebook page. We do not tolerate offensive language on our page at any time and I have therefore removed your comment on our post. I realise that this may well have been posted in error or that you may not have been aware of our policy but we would ask

you not to post in such a manner on our page again. Kind regards (name) Eastcott Community Organisation''

- will engage to further communication using the appropriate confidential messaging service supported by the social media platform.
- reserves the right to delete posts they deem offensive, inappropriate or detrimental to the centre.

6.4 Summary

The keys to success in social media are being honest about who you are, being thoughtful before you post, and respecting the purpose of the community where you are posting.

- protect confidential and proprietary information
- respect copyright and fair use
- don't us company logos on personal social media accounts
- clearly identify your opinions as your own
- Think twice
- Strive for accuracy
- Always be respectful
- Remember your audience. . . .

6.5 Dealing with phishing

There are various phishing techniques used by attackers:

- Embedding a link in an email that redirects you to an unsecure website that requests sensitive information
- Installing a Trojan via a malicious email attachment or advert which will allow the intruder to exploit loopholes and obtain sensitive information
- Spoofing the sender address in an email to appear as a reputable source and request sensitive information
- Attempting to obtain company information over the phone by impersonating a known company vendor or IT department

The following steps will be used to protect the Organisation against phishing:

- Educate volunteers and employees on phishing techniques.
- Ensure existing SPAM filters, that detects viruses, blank senders, etc, are enabled.
- Ensure all systems current with the latest security patches and updates.
- Install an antivirus solution and keep it up-to-date by monitoring the antivirus status on all equipment.
- Advise all volunteers and employees to use strong passwords. For advice on strong passwords please see: https://www.getsafeonline.org/protecting-your-computer/passwords/
- Deploy a web filter to block malicious websites.
- Encrypt all sensitive company information.

6.6 Data breach

When a breach is discovered, it is essential to act comprehensively and quickly, or it may expose the Organisation to greater liability. There are six critical steps the Organisation must take to deal with it.

It is important to bear in mind that these steps are not sequential – in practice, it will be necessary to think about most of them in parallel, particularly in the initial aftermath of the

breach where the priorities will be to contain it in order to mitigate any risk of further damage or loss of data.

- Inform chair of the Organisation
  The chair will ensure relevant people are involved in responding to the breach.
- Secure systems and ensure business continuity
  If the website is the cause of the breach secure it in order to contain the breach and ensure it is not on going.
- Conduct a thorough investigation
  Understand what went wrong and what steps will need to be taken to ensure it doesn't happen again
- Manage public relations
  notify the individuals concerned and manage announcements in an accurate, open and honest way.
- Address legal and regulatory requirements
  Identify which regulations have been broken and who needs to be notified.
- Incur liability
  Deal with any resulting financial liabilities

6.7 References

The following sites were used in creating this policy.

https://www.skidmore.edu/hr/policies/social-media.php

https://www.insight180.com/7-tips-for-responding-to-negative-comments-on-social-media/

https://digitalguardian.com/blog/phishing-attack-prevention-how-identify-avoid-phishing-scams

https://www.information-age.com/6-critical-steps-responding-cyber-attack-123459644/

7 Associated Policies

Policy Name	Policy Ref

8 Version Control

Version	V2.1		
Rational for changes	V2.0 Merge Social Media & Internet policies		
	V2.1 update Eastcott Community Organisation/Eastcott Community Centre Feb 2020		
Status	Approved		
Revision Author	Rebecca Campbell & Jo Innes		
Date Approved On	12 Nov 2018	Review Date	November 2019
Approved By			
Name	Role	Date of signature	
Committee		12th November (in minutes)	

Version 2.1
Status Approved
Dated Approved