Charity Number: 1160538
Policy Documentation

SOCIAL MEDIA AND INTERNET POLICY

Policy Reference	02
Status	Approved
Author	Caroline Davies-Khan
Revision Author	Arabella Thomas
Date Approved on	9th April 2018
Latest Review Date	14th July 2025

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 area of benefit
- 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 this threat.

2 Definitions

Term	Definition
Centre	The social hall managed by the Committee: Eastcott Community Centre, Savernake Street, Swindon, SN1 3LZ bookings@eastcottcommunity.org info@eastcottcommunity.org
Committee	The trustees who manage and run Eastcott Community Centre
Organisation	Eastcott Community Organisation
Phishing	A fraudulent attempt to obtain sensitive information via electronic communication. Such as emails, WhatsApp, Instagram or Facebook and other social media or electronic communication.
Social media	Platforms that allow users to share content or communicate online (e.g., Facebook, X/Twitter, Instagram, LinkedIn, YouTube).
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.
Personal Data	Information that identifies an individual, as defined under UK GDPR.

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

This policy applies to all trustees, staff, volunteers, and any other persons acting on behalf of the Organisation who use social media or access the internet in the context of their role, including but not limited to:

- Employees
- Trustees
- Volunteers

5 Legal and Regulatory Framework

This policy is aligned with the following legal standards:

- **UK General Data Protection Regulation (UK GDPR)**
- **Data Protection Act 2018**
- **Online Safety Act 2023**
- **Equality Act 2010**
- **Communications Act 2003 (as amended)**
- **National Cyber Security Centre (NCSC) guidelines**

6 Responsibilities

Role	Responsibility
Staff and Trustees	Oversee management of social media sites. Ensure a minimum of 2 administrators per site. Nominate which sites we have a presence on.
Administrators	To administer social media site in line with policy
All users	Must use good judgment, maintain respectful tone, and follow legal and organisational standards.

7 Policy

7.1 The Organisation

- Will follow the constitution, charitable objectives, and policies (especially confidentiality).
- Will keep social media accounts active and updated regularly.
- Will assign at least two volunteers per site to manage and respond to content.
- Will support relevant social media training for team members when needed.
- Will ensure messaging is consistent across all platforms.
- Will clearly identify themselves when posting on behalf of the Organisation.
- Will respect copyright by citing sources and seeking permissions.
- May share relevant content that aligns with community goals, with consideration for its impact.
- Will choose which platforms to engage with.
- Will use secure organisational passwords, shared with the staff and trustees.
- Will verify facts before posting.
- Will understand that posts may invite opposing views or discussion.
- Will remain mindful that social media content is publicly accessible.
- Will acknowledge and treat positive feedback appropriately.
- Will use email (not private messaging) to share personal or contact information.
- Will delete private messages from social media inboxes at least every 6 months.

7.2 Trustees, Employees and Volunteers:

- Will not represent the Organisation beyond its mission and objectives using their personal identity.
- Are responsible for the content they write and post.
- Must use good judgment and ensure posts do not reflect poorly on the Organisation.
- May post on behalf of the Organisation from personal accounts, but must clearly state their role (e.g., "I am a member of Eastcott Community Organisation…").
- Are free to use personal accounts as they choose but should use privacy settings if they do not wish to be associated with organisational content (e.g., tagging).
- Understand that using personal social media to air grievances about the Organisation may lead to action under the disciplinary and grievance policy.

7.3 Dealing with negative posts

The Organisation:

- Will not engage in arguments or "flame wars" — only respectful, civil discourse.
- Moderate posts for offensive, defamatory, or illegal content.
- May block, ban, or report users in cases of persistent, extreme, or illegal behaviour, following the Organisation's behaviour policy.
- Will ideally discuss moderation actions with the committee, but administrators or affected volunteers may act immediately if needed.
- Will use a standard, polite response when removing offensive posts, such as:

"I am writing to you in my capacity as [position] of Eastcott Community Organisation. We do not tolerate offensive language on our page and have removed your comment. Please refrain from posting in this manner again. Kind regards, [name]."

- Will continue any necessary communication using the platform's private messaging tools, where appropriate and secure.
- Reserves the right to delete posts deemed offensive, inappropriate, or harmful to the Centre's reputation.

7.4 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.

- Be honest about who you are.
- Think before you post and respect the community's purpose.
- Protect confidential and proprietary information.
- Always respect copyright and fair use.
- Do not use the Organizations' logos on personal accounts.
- Clearly state when opinions are your own.
- Think twice — be mindful of tone and timing.
- Strive for accuracy in everything you share.
- Always be respectful in all interactions.
- Remember your audience and the potential reach of your posts.

8 Phishing

8.1 Dealing with phishing

Phishing remains one of the most common forms of cyberattack and poses a serious risk to organisations. Attackers may use the following techniques to steal sensitive information or compromise systems:

- **Malicious Links in Emails**
  Emails may contain deceptive links that lead to fake websites designed to harvest login credentials, personal data, or payment details.
- **Malicious Attachments**
  Email attachments (e.g. PDFs, ZIP files, Office documents) may carry malware or Trojans that, once opened, install software allowing attackers to access sensitive data or control systems.
- **Email Spoofing**
  Cybercriminals often disguise their email address to appear as a trusted source, such as a colleague, vendor, or service provider, in order to trick users into sharing information or clicking harmful links.
- **Voice Phishing (Vishing)**
  Attackers may call impersonating legitimate organisations — such as IT support, banks, or suppliers — to extract confidential details or gain remote access to systems.

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 are 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.
- Only authorised individuals should have administrative access to systems and social media accounts.
- Advise all volunteers and employees to use strong passwords. For advice on strong passwords please see: https://www.getsafeonline.org/protecting-your-computer/passwords/
- Encourage all users to report suspicious emails or calls immediately to the Chair or IT contact and never respond directly.
- Deploy a web filter to block malicious websites.
- Encrypt all sensitive company information.

8.2 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.

- **Notify the Chair**
  The Chair will coordinate the response and involve all relevant personnel.
- **Secure Systems & Maintain Continuity**
  Immediately isolate affected systems (e.g. websites or devices) to contain the breach and prevent further impact.
- **Investigate the Incident**
  Identify the cause, scope, and nature of the breach. Document findings (policy breach log) and assess what went wrong.
- **Communicate Transparently**
  Notify affected individuals promptly and manage public communications with honesty and clarity.
- **Meet Legal Obligations**
  Identify which laws or regulations (e.g. UK GDPR) apply and notify the Information Commissioner's Office (ICO) within 72 hours if required.
- **Assess and Address Liability**
  Evaluate and manage any financial or legal consequences resulting from the breach.

9 References

The following sites were used in creating this policy:

Charity Number: 1160538
Policy Documentation

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/

https://www.gov.uk/data-protection

1 Associated Policies

Policy Name	Policy Ref
Data Protection	13

2 Version Control

Version	V3.0		
Rational for changes	V3.0 to update with latest legislation and guidance		
	V2.1 update Eastcott Community Organisation/Eastcott Community Centre Feb 2020 V2.0 Merge Social Media & Internet policies		
Status	Approved		
Revision Author	Arabella Thomas		
Date Approved On	14th July 2025		By Committee