ETNA Community Centre

...at the heart of TWI

Digital Policy – Artificial Intelligence & Social Media

Introduction

ETNA Community Centre is committed to using technologies, specifically Chat GPT 4 and social media platforms, to promote the Centre's activities. This policy sets out our principles and guidelines for the responsible use of AI, ensuring transparency, fairness, privacy, and accountability in all AI-related activities. It also provides clear parameters for staff, trustees and volunteers when utilising social media tools on behalf of ETNA or engaging in social media dialogue. The social media is managed by the Finance and Digital Coordinator (FDC) and overseen by the Centre Director.

Purpose

The purpose of this policy is to:

- Define the responsible use of AI technologies..
- Ensure compliance with all applicable laws and regulations, including data protection laws.
- Safeguard the privacy and rights of individuals interacting with AI systems.
- Promote transparency and accountability in AI-related decision-making processes.
- Minimise risks associated with AI misuse, bias, hacking, or sharing inappropriate content.
- Provide clear guidelines for the appropriate use of social media and AI by ETNA staff, trustees, and volunteers.
- Ensure all communications align with ETNA's values and mission.
- Establish procedures for proactive crisis management and addressing issues that may arise on social media.

Artificial Intelligence (AI)

Responsible AI Use

Ethical Considerations: ETNA will prioritise ethical considerations when using AI technologies. We will not use AI for any purpose that may harm individuals or communities whether users or prospective users of the Centre.

Transparency: We will provide clear and accessible information to users regarding the use of AI within our organisation, including the fact that we use Chat GPT 4.

Fairness: ETNA is committed to preventing and addressing bias in AI systems that may result in discrimination or unfair treatment of individuals or groups.

Data Privacy: We will uphold the highest standards of data privacy and security, ensuring that personal data is protected in accordance with applicable data protection laws.

Data Handling and Security

Data Collection: ETNA will only collect and use data that is necessary for the operation of AI systems. Data collection will be done with user consent and in compliance with relevant data protection regulations.

Data Security: We will implement robust security measures to protect AI-related data from unauthorised access, breaches, and misuse.

Data Retention: ETNA will retain AI-related data for only as long as necessary, and we will regularly review our data retention policies.

Accountability and Governance

Responsibility: We will designate responsible individuals within our organisation to oversee AI initiatives, monitor their performance, and ensure compliance with this policy.

Bias Mitigation: We will regularly assess and address biases in AI systems to ensure fair and equitable outcomes.

Compliance: We will stay up to date with relevant laws, regulations, and ethical guidelines related to AI and ensure compliance with them.

Training and Education

Awareness: ETNA will educate its staff and volunteers about the responsible use of AI technologies, including the potential ethical challenges and risks.

Continuous Learning: We will stay informed about the latest developments in AI ethics and best practices to adapt our policies accordingly.

Complaints and Feedback

ETNA welcomes feedback and complaints related to the use of AI. We will provide clear channels for individuals to express concerns, and we will investigate and address them promptly and appropriately.

Social Media

Using ETNA's social media channels — appropriate conduct

1. As an employee and representative of ETNA you are expected to demonstrate best practices and appropriate etiquette on social media, including but not limited to the following:
   - Be respectful to all.
   - No hate speech.
   - Do not share confidential charity information.
   - Do not share personal opinions or engage in any political or other debates either directly by commenting or indirectly by 'liking', 'sharing' or 'reposting'. If you are in doubt about ETNA's position on a particular issue, please speak to the CD or Chair.
2. Ensure all social media content has a purpose and a benefit for ETNA, and accurately reflects the charity's agreed position. To be an ambassador for the charity ensuring ETNA's values are reflected in what is posted and the tone of voice.
   - a call to action.
   - sharing of events/activities.
   - re-posting of other community events as long as they are non-political/non-offensive/relevant.
3. Any video content/images of people must have the necessary permissions in writing before being used. All relevant rights for usage must be obtained before publishing material. It is critical that all images and text abides to copyright law.
4. **Always pause and think before posting**. If replying to comments respond in a timely manner, when a response is appropriate.
5. Take care with the presentation of content. Make sure that there are no typos, misspellings, or grammatical errors. Also check the quality of images.
6. Always check facts. Staff should not automatically assume that material is accurate and should take reasonable steps where necessary to seek verification, for example, by checking data/statistics and being wary of photo manipulation. Check if re-posting the authenticity/appropriateness of the client's account.
7. ETNA is not a political organisation and does not hold a view on party politics or have any affiliation with or links to political parties. Care should be used during pre-election periods (PURDAH) to ensure that no political bias is shown or implied.
8. Monitor social media accounts for 'tagging/mentions' and if necessary, block and report.

The Centre Director and FDC are responsible for setting up and managing ETNA's social media channels. Only those authorised to do so will have access to these accounts. No other groups or accounts should be opened in the charity's name. If a new platform is to be considered this must be signed off by the Centre Director.

It is all staff and volunteers' responsibility to be vigilant and act responsibly when accessing ETNA's accounts on their personal devices.

Complaints and Issues

If a complaint is made on ETNA's social media channels, staff should seek advice from the Centre Director or Chair of Trustees before responding. If they are not available, then staff should speak to the Office Manager.

Sometimes issues can arise on social media which can escalate into a crisis situation because they are sensitive or risk serious damage to the charity's reputation. Examples might include ETNA being linked to a group that is behaving illegally or against the morals of the charity. The nature of social media means that complaints are visible and can escalate quickly. Not acting can be detrimental to the charity.

In a crisis it is important that both the Chair of Trustees and Centre Director are informed and they will work closely with the team member to ensure that a plan of action for responding to the situation is put in place. This may involve taking advice from Richmond CVS or other parties.

Hacking

The other risk to ETNA is if one of the social media accounts is hacked.
Passwords must be updated every 3 months and not shared.

Red Flags of a Hacked Social Media Account

- Strange posts or messages on your account that you didn't write.
- Account password suddenly changes, and you can't log in.
- Strange messages or friend requests from people you don't know.
- Account settings are changed, and you can't change them back.
- Profile picture has been changed without your knowledge.
- Spam messages or comments on your posts.
- Account is suddenly deactivated or suspended for no apparent reason.
- Unable to log in to your account from a different device or location.
- An error message when you try to log in, even though you're using the correct password.
- People tell you they've been receiving strange messages from your account.

Immediate Actions

- Change password to a strong unique password that hasn't been used before and communicate with team what has happened.
- Change passwords across other social media platforms etc.
- Enable multi-factor authentication.
- Report to the social media platform.
- Review account settings and change them back, if necessary.
- Check profile picture and change it back.
- Delete any strange messages or posts from the account.
- Unfriend or block any suspicious users.
- Contact customer support if having problems logging in.
- Be extra careful with personal information and identity theft.
- Notify the Centre Director immediately.

Review and Update

This policy will be reviewed periodically to ensure its continued relevance and effectiveness in line with the evolving landscape of AI technologies and social media platforms.

Date of policy: **September 2024**

Next review: **September 2025**