



SOCIAL MEDIA POLICY

REVIEWED: November 2024

NEXT REVIEW: November 2025

1. Statement

1.1. This policy is intended to help staff make appropriate decisions about the use of social media such as (but not limited to) blogs, wikis, social networking websites, podcasts, forums, message boards, or comments on web-articles, such as Twitter, Facebook, LinkedIn etc.

1.2. This policy outlines the standards we require staff to observe when using social media, the circumstances in which we will monitor your use of social media and the action we will take in respect of breaches of this policy.

2. Who is Covered?

2.1. This policy covers all individuals working at all levels and grades, including senior managers, employees, and volunteers (collectively referred to as **staff** in this policy).

3. Scope

3.1. All staff are expected to comply with this policy at all times to protect the privacy, confidentiality, and interests of our organisation and our services, employees, service users and partners.

3.2. Breach of this policy may be dealt with under our disciplinary procedure (set out in the Capability, Disciplinary and Grievance Policy) and, in serious cases, may be treated as gross misconduct leading to dismissal.

4. Responsibility for Implementation

4.1. The Chief Executive has overall responsibility for the effective operation of this policy. The terms of the policy are to be reviewed and agreed by the Risk, Policy & Safeguarding sub group of the Board.

4.2. The Deputy CEO is responsible for monitoring and reviewing the operation of this policy and making recommendations for changes to minimise risks to our operations.

4.3. All staff are responsible for their own compliance with this policy and for ensuring that it is consistently applied. All staff should ensure that they take the time to read and understand it. Any breach of this policy should be reported to the Chief Executive or the Deputy CEO.

4.4. Questions regarding the application of this policy should be directed to the Chief Executive or Deputy CEO.

4.5. Questions regarding the content of this policy should be directed to the Risk, Policy & Safeguarding sub group of the Board.

5. Using Social Media Sites in our Name

5.1. Only designated staff are permitted to post material on a social media website in our name and on our behalf. Any breach of this restriction will amount to gross misconduct. Designation will be granted by the Chief Executive.

6. Using Work-Related Social Media

6.1. We recognise the importance of the internet in shaping public thinking about our organisation and our services, employees, partners and service users. We also recognise the importance of our staff joining in and helping shape conversation and direction through interaction in social media.

6.2. Before using work-related social media you must:

(a) have read and understood this policy

and

(b) have sought and gained prior approval to do so from your Line Manager as set out in your job description

and

(c) have provided your line manager with your password and set the account up using your work email address.

7. Rules for Use of Social Media (as a designated member of staff for the organisation)

Whenever you are permitted to use social media in accordance with this policy, you must adhere to the following general rules:

7.1. Do not upload, post, forward or post a link to any abusive, obscene, discriminatory, harassing, derogatory or defamatory content.

7.2. Any member of staff who feels that they have been harassed or bullied, or are offended by material posted or uploaded by a colleague onto a social media website should inform the Chief Executive.

7.3. Never disclose sensitive, private or confidential information. If you are unsure whether the information you wish to share falls within one of these categories, you should discuss this with the Chief Executive or Deputy CEO.

7.4. Do not upload, post or forward any private or personal content belonging to a third party unless you have that third party's consent.

7.5 When making use of any social media platform, you must read and comply with its terms of use.

7.6. Do not post, upload, forward or post a link to chain mail, junk mail, inappropriate cartoons, jokes or gossip.

7.7. Be honest and open, but be mindful of the impact your contribution might make to people's perceptions of us as an organisation. If you make a mistake in a contribution, be prompt in admitting and correcting it.

7.8. You are personally responsible for content you publish into social media tools – be aware that what you publish will be public for many years.

7.9. Don't escalate heated discussions, try to be conciliatory, respectful and quote facts to lower the temperature and correct misrepresentations. Never contribute to a discussion if you are angry or upset, return to it later when you can contribute in a calm and rational manner.

7.10. If you feel even slightly uneasy about something you are about to publish, then you shouldn't do it. If in doubt, always discuss it with the Chief Executive or Deputy CEO first.

7.11. Always consider others' privacy and avoid discussing topics that may be inflammatory e.g. politics and religion.

7.12. Avoid publishing your contact details where they can be accessed and used widely by people you did not intend to see them, and never publish anyone else's contact details.

7.13. Activity on social media websites during office hours should complement and/or support your role and should be used in moderation.

7.14. Before posting any photographs on social media websites, staff must confirm that permission is in place - this is especially true when dealing with photographs or information relating to young people.

8. Rules for Use of Social Media (in a personal capacity)

Whenever you use social media you enter the public domain as a representative of NE Youth, therefore you must adhere to the following general rules:

8.1. Never interact with service users of NE Youth using personal social media.

8.2 Do not upload, post, forward or post a link that may be construed as offensive, illegal, discriminatory or abusive.

8.3. Do not upload, post, forward or post a link that may be construed as offensive, illegal, discriminatory or abusive towards or against NE Youth or its employees.

8.4. Any member of staff who feels that they have been harassed or bullied, or are offended by material posted or uploaded by a colleague onto a social media website should inform the Chief Executive.

8.5. Never post private or confidential information relating to NE Youth.

8.6. When making use of any social media platform, you should always read and comply with its terms of use.

8.7. Be honest and open, but be mindful of the impact your contribution might make to people's perceptions of us as an organisation. If you make a mistake in a contribution, be prompt in admitting and correcting it.

8.8. You are personally responsible for content you publish into social media tools – be aware that what you publish will be public for many years.

9. Monitoring Use of Social Media Websites

9.1. Staff should be aware that use of the organisation's social media websites will be monitored and, where breaches of this policy are found, action may be taken under our disciplinary procedure (set out in the Capability, Disciplinary and Grievance Policy)

9.2. In particular uploading, posting forwarding or posting a link to any of the following types of material on a social media website, whether in a professional or personal capacity, will amount to gross misconduct (this list is not exhaustive):

(a) pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);

(b) a false and defamatory statement about any person or organisation;

(c) material which is offensive, obscene, criminal discriminatory, derogatory or may cause embarrassment to us, our service users or our staff;

(d) confidential information about us or any of our staff or service users (which you do not have express authority to disseminate);

(e) material in breach of copyright or other intellectual property rights, or which invades the privacy of any person.

9.3. Where evidence of misuse is found we may undertake a more detailed investigation in accordance with our disciplinary procedure (set out in the Capability, Disciplinary and Grievance Policy) involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the investigation. If necessary such information may be handed to the police in connection with a criminal investigation.

9.4. If you notice any use of social media by other members of staff in breach of this policy please report it to the Chief Executive or Chairman of the Board of Directors

Crisis communications

A crisis is defined as any event that can cause harm to NE Youth's reputation. If an incident occurs that could generate media interest, this crisis communications team will meet to agree a position statement and key messages, and follow all media protocols.

In the event of a crisis, the crisis communications team (which will be convened by the CEO/or the Deputy CEO where appropriate and in line with the Crisis Communications Plan) is responsible for:

- liaising with the senior management team/crisis response team
- managing all media and social media statements, press releases, interviews and media visits as appropriate
- monitoring press/media coverage and taking action as required
- managing internal communications, utilising the guidance of our external HR provider if required
- advising on actions necessary to protect NE Youth's reputation

Individual staff, volunteers and trustees who are not members of the crisis communications team should not respond to any social media posts or requests for information. Any such posts or requests such be directed as soon as possible to the Chief Executive or the Business Development Manager for action.