

Social Media and Public Relations

Scope

- **Policy Statement**
- **The Policy**
- **Handling a Media Enquiry**
- **Media Statements**
- **Press Releases**
- **Interview Reports**
- **Requests from Police**
- **Confidentiality and Consent**
- **Procedures for Employees**
- **Social Media and Networking**
- **Related Policies**
- **Related Guidance**
- **Training Statement**
- **MEDIA CONSENT FORM**

Policy Statement

The company takes seriously its responsibility to convey and reflect, within the public domain, a professional response to any media-led interest in our activities. This policy sets out the key principles which govern contact with any media enquiry received by the company. We recognise that in today's fast moving digital communication world there is a significant role played by any media interest or coverage in people's perceptions and of the effect such perceptions can have on our business.

This policy also provides guidance for employee use of social media, which should be broadly understood for purpose of this policy to include blogs, wikis, microblogs, message boards, chat rooms, electronic newsletter, online forum, social networking sites, and other sites and services that permit users to share information with others in contemporaneous manner.

The Policy

Handling a Media Enquiry

Should any member of staff be approached by local or national journalists, or, free-lance writers, they should respond with "no comment" and immediately pass the enquiry to Head/Deputy HR or Social Media Department. This person is responsible for responding to the enquiry and will make a judgement about any advice which might need to be sought before the response is forthcoming.

Media Statements

These are generally a written response to articles, complaints or a regulatory visit, any media statement must be approved and signed off by a Director prior to release.

Press Releases

These are used as the main way to highlight good news stories. They can include stories on staff awards/achievements, fund raising or grant awards for specific areas of work e.g. dementia etc. Advertorials are used in much the same way. All press releases must only be compiled, edited and released by (Director, Marketing Director, Press Officer – delete as necessary) unauthorised publishing will be subject to disciplinary action.

Interview Reports

Such requests are sometimes accompanied by requests for access to film or photographs. This is usually in response to a proactive press release, or, in reaction to an unplanned story. All such requests must be approved, appropriate consent sought where required and forwarded to the appropriate person [Insert Here Job Title]. Staff need to exercise caution if approached whilst on duty in the event of reporters posing as someone else (undercover), if they suspect this to be the case, they should report it immediately to their manager or Director. Any requests involving service users are subject to the usual safeguarding controls i.e. consent, capacity to consent, family or best interest decision considerations and duly recorded.

Requests from police

These are usually received when the Police require assistance from the public to progress a criminal investigation. These need sensitive handling, particularly where a service-user is a victim of the crime. The usual safeguarding controls should be actively in place and followed before any approval is given.

Confidentiality and Consent

The usual rules of sharing information must be adhered to and are particularly relevant where the situation is still ongoing e.g. complaint investigation, disciplinary action, criminal investigation and where necessary any discussions between multi-agency partners as to who is best placed to make the response. Only the authorised officer from each organisation will be permitted to discuss and agree the response.

Procedure for Employees – Social Media and Networking

- Employees are required to understand and follow the Skills for Code of Conduct and Employee Handbook.
- Employees should be aware of the effect their social media postings could have on their reputation, as well as this organisation's reputation when posting on the organisation's social media, as the information that employees post or publish may be public information for a long time.
- If unsure, don't post, employees should err on the side of caution when posting to social networks
- If an employee feels an update or message might cause complaints or offence or be otherwise unsuitable, they should not post it, employees can always consult management for advice.
- Be thoughtful and polite, many social media users have got into trouble simply by failing to observe basic good manners online.
- Employees should adopt the same level of courtesy used when communicating via email.
- Look out for security threats, employees should be on guard for social engineering and phishing attempts.
- Social networks are also used to distribute spam and malware.

Employees should be aware that this organisation might view content and information made available by employees through social media

Posting on the organisation's social media

- Only those employees who are authorised must post on the organisation's social media.
- Users must not:
 - Create or transmit material that might be defamatory or incur liability for the Company.
 - Publish content not in line with the organisation's mission and ethos
 - Post messages, status updates or links to material or content that is inappropriate. Inappropriate content includes (but is not limited to): pornography, libellous, discriminatory material, or material that can create a hostile work environment, racial or religious slurs, gender-specific comments, information encouraging criminal skills or terrorism, materials relating to cults, gambling and illegal drugs and/or material that breaches any confidentiality of the organisation, employees or service users.
 - This definition of inappropriate content or material also covers any text, images or other media that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristics protected by law.
 - Use social media for any illegal or criminal activities.
 - Send offensive or harassing material to others via social media.
 - Broadcast unsolicited views on social, political, religious or other non-business-related manners.
 - Send or post messages or material that could damage the organisation's image or reputation.

- Interact with the organisation's competitors in any ways which could be interpreted as being offensive, disrespectful or rude.
- Post, upload, forward or link to spam, junk email or chain emails and messages.
- If an employee is uncertain about what would be appropriate to post under this policy, they should check with their supervisor or manager.
- If any social media network, blogs and/or other types of online content generate press and media attention or legal questions, employees should refer these enquiries to their manager or appropriate person in this organisation.
- In general, employees should only post updates, messages or otherwise use these company accounts when that use is clearly in line with the organisation's overall objectives.
- If employees find or encounter a situation while using social media that threatens to become antagonistic, employees should disengage from the dialogue in a polite manner and seek the advice of their supervisor or manager.
- Employees should get appropriate permission before they refer to or post images of current or former employees, service users or their families, members, vendors or suppliers.
- Additionally, employees should get appropriate permission to use a third party's copyright, copyright material, trademarks, service marks or other intellectual property.
- Social media use should not interfere with the employee's responsibilities.
- The computer systems, office mobile phones or land lines are to be used for business purposes only.

Using personal social media accounts

- Employees must not post any commentary, information, content, or images on any personal social media in connection with, or which could be interpreted to be about, the organisation or any of its employees or service users.
- Employees must not refer to their employment at the organisation on any personal social media sites, save for LinkedIn or other business networking site where they have the permission of their manager to do so.
- If an employee has permission to refer to their employment at the organisation on LinkedIn or another business networking site, then they must observe the rules contained in the section above entitled '*Posting on the organisation's social media*'.
- During working time, whether on the organisation's computer system or the employee's own device, for example their mobile telephone, personal use of social media networks or personal blogging of online content is forbidden and could result in disciplinary action.
- The Company is not responsible for the individual actions of the employees.

Any online activity that violates the organisation's Code of Conduct or any other company policy may subject an employee to disciplinary action or termination of their

contract. This policy will be implemented and monitored by all managers throughout the organisation.

Related Policies

Adult Safeguarding
Code of Conduct for Workers
Confidentiality
Cyber Security
Data Protection Legislative Framework (GDPR)
Good Governance
Monitoring and Accountability

Related Guidance

- Get Safe Online www.getsafeonline.org
- Cyber Aware www.cyberaware.gov.uk

Training Statement

All staff, during induction are made aware of the organizations policies and procedures, all of which are used for training updates. All policies and procedures are reviewed and amended where necessary and staff are made aware of any changes. Observations are undertaken to check skills and competencies. Various methods of training are used including one to one, on-line, workbook, group meetings, individual supervisions and external courses are sourced as required.