VIEWPOINT
joy in later years

Approver	Board
Date Approved	February 2020
Classification	Policy
Title	Social Media Policy
Revision Date	March 2023
Revised by	Director of Finance & Business Support
Next Revision Date	March 2026
Related Documents	ICT Systems Security Policy & Procedures; Privacy Policy; Code of Conduct for Staff; Disciplinary Policy & Procedures
Location of Electronic Copy	F:\Live Policies\Corporate

1. Policy Statement

Viewpoint encourages the use of its electronic information and communication technology and related systems to aid communication and improve efficiency of working practices. However, inappropriate use of our systems can cause serious problems that may involve legal claims against both the organisation and against individual users.

This policy is in place to minimise the risks to our business through use of social media.

This policy deals with the use of all forms of social media, including Facebook, LinkedIn, Twitter, Google, Wikipedia, Instagram, Tumblr and all other social networking sites, internet postings and blogs. It applies to use of social media for business purposes as well as personal use that may affect our business in any way.

This policy does not form part of any employee's contract of employment and we may amend it at any time.

2. Purpose

This policy deals mainly with the use of Social Media and sets out the standards that users of our systems are expected to observe.

It complements and should be read in conjunction with the ICT Systems Security Policy & Procedures, which sets out the requirements of employees when using all of our electronic communication systems and equipment for both business and personal use.

'Business use' is defined as access to, or publishing of content on any social media site which results in a clear business benefit.

'Personal use' is defined as access to, or publishing of content on any social media site for which employees are pursuing their own interests and for which there is no clearly defined business benefit.

3. Legislation/ related policies

Use of Viewpoint Systems is likely to involve the processing of personal data and is therefore regulated by the Data Protection Act 2018 together with the Employment Practices Data Protection Code, issued by the Information Commissioner.

Professional bodies such as the SHR, Care Inspectorate, NMC and SSSC have regulations and Codes of Conduct for employees registered with them, concerning confidentiality and the use of social media, which must be adhered to by Viewpoint employees.

Social media should never be used in a way that breaches any of our other policies. If an internet post would breach any of our policies in another forum, it will also breach them in an online forum. For example, you are prohibited from using social media to:

- breach our ICT Systems Security Policy or Procedures;
- breach our obligations with respect to the rules of relevant regulatory bodies;
- breach any obligations contained in those policies relating to confidentiality;
- breach our Disciplinary Policy or procedures;
- harass or bully other staff in any way OR breach our Code of Conduct for Staff;
- unlawfully discriminate against other staff or third parties;
- breach our Privacy Policy (for example, never disclose personal information about a colleague online); or
- breach any other laws or regulatory requirements.

Staff should never provide references for other individuals on social or professional networking sites, as such references, positive or negative, can be attributed to the organisation and create legal liability for both the author of the reference and the organisation.

Staff who breach any of the above policies will be subject to disciplinary action up to and including termination of employment.

4. Scope

This policy applies to all individuals working for Viewpoint at all levels.

Social networking

We respect your right to a private life and that includes joining any social sites you want. However, information posted on these sites is classed as public and not private. As a result, you are not allowed to reveal confidential information relating to us, our customers, partners, suppliers, board members, employees and so on. You are also not allowed to post any comments on people and events connected to us, or make any remarks which could possibly bring us into disrepute. Any actions could result in disciplinary action, including dismissal.

Policy for business use of social media

The CEO has overall authority with regard information about Viewpoint's business posted on social media. Where there is a clear business benefit, specific staff members and volunteers will be granted social media access on behalf of Viewpoint. The Executive is responsible for deciding which social media sites we should use for business purposes and individual usage will be monitored.

Staff members using social media need to ensure that their use complies with all of the provisions of our ICT Systems Security Policy & Procedures.

Those using social media on behalf of Viewpoint are expected to use common sense and ensure that all of our interactions are positive and uphold our reputation. They are also expected to always ensure that any information published on these websites has been through the necessary checks for accuracy and complies with our Privacy Policy.

If your duties require you to speak on behalf of the organisation in a social media environment, you must still seek approval for such communication from your line manager, who may require you to undergo training before you do so and impose certain requirements and restrictions with regard to your activities.

Likewise, if you are contacted for comments about the organisation for publication anywhere, including in any social media outlet, direct the enquiry to a member of the Executive team and do not respond without written approval.

The use of social media for business purposes is subject to the remainder of this policy.

Policy for personal use of social media

We trust our staff to represent Viewpoint well even outside working hours and to be sensible in your own use of Social Media. Here are some recommendations:

- ✓ You should make it clear in social media postings, or in your personal profile, that you are speaking on your own behalf. Write in the first person and use a personal email address.
- ✓ Be mindful of how you represent yourself on social networks as the lines that differentiate between what is public or private and what is personal or professional are becoming increasingly blurred.
- ✓ Be aware that social networking websites can act as public forums, and that 'confidential' areas of these sites may not have reliable security controls.
- ✓ Be respectful to others when making any statement on social media and be aware that you are personally responsible for all communications which will be published on the internet for anyone to see.
- ✓ If you identify yourself as working for Viewpoint in social networks you must state that your views do not represent those of your employer (unless you are authorised to speak on our behalf as set out in paragraph 3) and ensure that content associated with you as an identifiable Viewpoint employee is consistent with your role in the organization and does not compromise our reputation or values.
- ✓ Remember that you may be connected or visible to Viewpoint colleagues, members and partners unless you go to extraordinary lengths to keep your online content private. Be sure to manage what information you are sharing and with whom.

- ✓ Do not make information available that could provide a person with unauthorised access to commercially sensitive and/or confidential information.
- ✓ Do not comment on work related issues or on our business.
- ✓ Do not set up personal use groups, blogs or any other form of social media which is Viewpoint branded, contains content for which we own the copyright or which could be linked with Viewpoint.
- ✓ Always use your personal email address and not your work address to set up social media accounts.
- ✓ If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from posting it until you have discussed it with your line manager.
- ✓ If you see social media content that disparages or reflects poorly on us, you should contact your line manager in the first instance.

Prohibited use

You must avoid making any social media communications that could damage our business interests or reputation, even indirectly.

You must not use social media to defame or disparage us, our staff or any third party; to harass, bully or unlawfully discriminate against staff or third parties; to make false or misleading statements; or to impersonate colleagues or third parties.

You must not express opinions on our behalf via social media, unless expressly authorised to do so by your line manager. You may be required to undergo training in order to obtain such authorisation.

You must not post comments about sensitive business-related topics, such as our performance, or do anything to jeopardise our trade secrets, confidential information and intellectual property. You must not include our logos or other trademarks in any social media posting or in your profile on any social media.

You are not permitted to add business contacts made during the course of your employment to personal social networking accounts.

5. Compliance & Support

Individuals using our ICT systems are required to maintain standards of honesty and integrity at all times. All members of staff are required to sign the ICT Systems Security Policy & Procedures.

Breach of this policy may result in disciplinary action up to and including dismissal. Any member of staff suspected of committing a breach of this policy will be required to co-operate with our investigation.

You may be required to remove any social media content that we consider to constitute a breach of this policy. Failure to comply with such a request may in

itself result in disciplinary action

6. Monitoring & Evaluation

Viewpoint reserves the right to audit and monitor, intercept and review, without further notice, staff activities using our ICT resources and communication systems. Including but not limited to social media postings and activities, for legitimate business purposes which include ascertaining and demonstrating that expected standards are being met by those using the systems and for the detection and investigation of unauthorised use of the systems (including where this is necessary to prevent or detect crime. We reserve the right to access, at any time, any computer file, data file, log file, document, voicemail message, email message or mailbox to maintain and protect the systems for the benefit of Viewpoint.

This policy will be reviewed by the board every 3 years.