
Social Media
Behance
Facebook
LinkedIn
Instagram
Pinterest
WhatsApp
TikTok

National Policy ☒ National Procedure ☐ National Protocol ☐ National Guideline ☐

National Clinical Guideline ☐

HSE National Policy for Social Media and Data Protection Staff Use

DOCUMENT GOVERNANCE [1]	
Document Owner (post title):	National Director of Communications National Director for Public Involvement, Culture and Risk Management and Chief Risk Officer
Document Owner name:	Mark Brennock Joe Ryan
Document Owner email contact:	DPO@hse.ie digital@hse.ie
Document Commissioner(s): (Name and post holder title):	Muiriosa Ryan Social Media Manager
Document Approver(s): (Name and post holder title):	Mark Brennock Joe Ryan
Development Group Name:	Social media, data protection working group
Development Group Chairperson:	Muiriosa Ryan

DOCUMENT MANAGEMENT [2]			
Date effective from:		01/09/2025	
Date set for next review:		31/08/2028	
Current version no:	2	**Archived version no:**	1

VERSION CONTROL UPDATE [3]		
Version No.	**Date Reviewed**	**Comments**
2	01/09/2025	Change from a guideline to a policy and more detail on data protection in doc. V2 titled “HSE national policy for Social Media and Data Protection Staff Use”
1	31/10/2023	Change from a 6 to a 7 page document. V1 titled “HSE Social Media Staff Use Guidelines”
0	01/01/2022	Original publication

[1] Records the senior management roles involved in the governance and development of the document.
[2] Records the control information about the document.
[3] Records details when a document is reviewed, even if no changes are made.

PUBLICATION INFORMATION [4]
Topic
Social Media and Data Protection Staff Use Policy
National Group
Social media and data protection working group
Short summary:
It is the policy of the HSE to share best practice when posting on social media and digital channels whether in a professional or personal capacity. The document also serves as a framework for responsible use of recording devices and the use of social media in HSE settings.
Description:
The purpose of this policy is to raise awareness for HSE staff to protect patient confidentiality, uphold professional standards, and ensure that personal freedoms are respected while lessening any risks associated with social media use in the workplace. The policy applies to the use of recording devices, and social media for professional purposes, as well as personal use that may affect our organisation in any way. This document does not serve to replace the role of the HSELive team, but to advise individual staff members on how social media can be used to support or enhance their work.

[4] Records the document information required for publication on the HSE National Central Repository.

1.0 Planning

1.1. Purpose

The purpose of this policy is to raise awareness for HSE staff to protect patient confidentiality, uphold professional standards, and ensure that personal freedoms are respected while lessening any risks associated with social media use in the workplace.

The policy applies to the use of recording devices, and social media for professional purposes, as well as personal use that may affect our organisation in any way.

1.1.1. Target users

Applies to all HSE staff (approx. 148,000 staff members) and covers both professional and personal use of social media.

1.1.2. Target population

HSE staff

1.4. Objective(s)

- Protect patient data and confidentiality.
- Maintain the integrity and reputation of the HSE.
- Provide clear guidelines on acceptable use of recording devices and social media.
- Educate service users and staff on appropriate use and risks.
- Reduce legal and reputational risks associated with misuse.

1.5. Outcome(s)

- Improved data protection compliance.
- Reduced incidents of inappropriate social media use.
- Enhanced patient confidentiality and staff awareness.
- Consistent national guidance for staff.

1.1. Rationale / alignment with HSE national priorities

The policy responds to the increased use of digital channels and recording devices. It aligns with GDPR obligations and HSE priorities to protect patient confidentiality, ensure responsible communication, and uphold organisational reputation in the digital age.

1.2. Supporting evidence

- General Data Protection Regulation (GDPR)
- HSE Data Protection Policy
- HSE Grievance and Disciplinary Procedure
- Guide to Professional Conduct and Ethics for Registered Medical Practitioners (2024)

2.0 Methodology

The development of the policy was led by the Social Media and Data Protection Working Group, including representatives from HSE Communications, the Data Protection Office, and Digital teams.

2.1.1. List of key questions this National 3PG will answer

- How should staff use social media professionally and personally to comply with GDPR?
- What constitutes appropriate vs inappropriate use of social media in a healthcare context?
- How should patient recordings be managed within GDPR guidelines?
- How should HSE respond to public social media posts that may contain patient information?

2.2. Describe and document the evidence search

The policy reflects legislative requirements under GDPR, HSE internal policies, and real-world examples of social media misuse in healthcare. The group reviewed HSE guidance, legal obligations, and best practice examples to produce clear operational guidance. No external copyright permissions were required.

2.4. Attach any copyright or permissions sought

No copyright or permissions are required in relation to this document.

3.0 Consultation

3.1. Stakeholder involvement

The development group included Communications, Digital, and Data Protection representatives. The policy reflects input from frontline staff, data protection officers, and communications leads. It was developed with consideration of how staff engage with patients and the public in digital spaces.

3.2. External review

Review was conducted by HSE Communications leadership and Data Protection experts. Their relevant expertise in compliance and digital communications informed the final draft prior to submission for governance approval.
The document was reviewed and approved by HSE Senior Leadership Team in August 2025.

4.0 National implementation plan

4.1. Describe the structure and governance of the national implementation team.

Monthly social media training session available on request.

4.2. List tools and resources developed to support local implementation of the National 3PG.

Monthly social media training session available on request.

5.0 Governance and approval

The governance and approval arrangements rest with National Director of Communications and National Director for Public Involvement, Culture and Risk Management and Chief Risk Officer. The Social Media and Data Protection Staff Use Policy was commissioned by Muiriosa Ryan, Social Media Manager. Following development of the National document, a Checklist was used in assessing that the National document met the standards outlined in How to Develop HSE National PPPGs – A Practical Guide, and signed and dated by the Chairperson of the Development Group.

The Social media and data protection working group recommended the National document to Senior Leadership Team with a signed and dated copy of the Checklist. The Social media and

data protection working group) submitted the final document and Checklist to National Directors for sign off.

6.0 Communication and dissemination plan

There will be an article in the Winter Edition of Health Matters, due to be published in December 2025. There will be an all staff broadcast alerting staff to the policy. There will be a LinkedIn post, targeting HSE staff letting them know the policy is on the website.

The document can be accessed only on the HSE National Central Repository, the single trusted source for accessing, storage and document control for all National PPPGs and National Clinical Guidelines. No duplicate copies of the National document should be accessible in any secondary electronic locations, only the link to the document on the Repository should be used on other locations. This link will automatically update in all locations if changed on the Repository.

7.0 Review of National Document

This National document will be reviewed every three years unless there is any new supporting evidence identified by findings from audit and evaluation, advances in technology or research, then the National document should be reviewed, updated and published as necessary.

Appendix 1: Membership of Development Group

Membership of social media and data protection working group	
Ben Cloney	Assistant National Director
Mary Deasy	Data Protection Officer
Muiriosa Ryan	Social Media Manager
Laura Monaghan	Senior Communications Manager
Agata O'Reilly	DPO Transformation Programme
Johnny Farren	Data Protection Office Support
Tara Looney	Head of Digital

Membership of social media and data protection approval governance group	
Mark Brennock	National Director of Communications
Joe Ryan	National Director for Public Involvement, Culture and Risk Management and Chief Risk Officer

Sign-off by Chair of Approval Governance Group

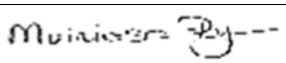
Name	Muiriosa Ryan
Title	Social Media Manager
Signature	

Table of Contents

Purpose

The purpose of this document is to inform HSE staff of best practice when posting on social media and digital channels whether in a professional or personal capacity. The document also serves as a framework for responsible use of recording devices and the use of social media in HSE settings.

The Digital Age provides us all with an opportunity to communicate widely in real-time and across multiple digital channels and devices. We can share content, opinions and third-party information. But with this opportunity comes a responsibility to respect others, share facts only and always remain courteous.

Social media provides the HSE with an opportunity to communicate with members of the public. Our customer service team, HSELive and social media team, manage all public-facing queries via the existing channels of phone, email, social media and Live Chat.

By following the policy, service users and visitors should be informed of the rules around using social media in a HSE setting. As well as this, the policy will help HSE staff to protect patient confidentiality, uphold professional standards, and ensure that personal freedoms are respected while lessening any risks associated with social media use in the workplace.

The policy applies to the use of recording devices, and social media for professional purposes, as well as personal use that may affect our organisation in any way.

This document does not serve to replace the role of the communications or data protection teams, but to advise individual staff members on how social media can be used to support or enhance their work.

Scope

The scope of this policy is applicable to all the HSE's 148,000 staff and includes professional and personal use of social media.

This policy should be read in conjunction with other related HSE policies, namely:

- Data Protection Policy here
- HSE Grievance and Disciplinary guidelines available here
- Guide to Professional Conduct and Ethics for Registered Medical Practitioners here

Part 1

Social media and professional use

Part 1: Social media and professional use

Social media channels can be set up by individual HSE departments. You can contact the social media team for further guidance and advice on this at digital@hse.ie

If you are using social media in a professional capacity, please adhere to the best practice guidelines.

Part 2

Data protection and social media

Part 2: Data protection and social media

Objectives

- To protect patient data and confidentiality.
- To maintain the integrity and reputation of the HSE.
- To provide clear guidelines on acceptable recording devices and social media use.
- To educate service users on the appropriate use of recording devices.
- To educate staff on the potential risks and consequences of social media misuse.

Recording devices

For the purposes of this policy, a recording device is any electronic device used to capture and store audio and video, typically mobile phones, but can also include the following:

Audio recorders:
Devices like mobile phones, voice recorders, dictation machines, and digital audio recorders.

Video recorders:
Devices like mobile phones, cameras, camcorders, and other devices that capture video footage.

When it is appropriate for staff to post on social media

HSE endorsed accounts:

- Staff may use official HSE social media accounts to share information about health services, campaigns, and public health messages.
- Example: Posting updates about vaccination drives or health awareness campaigns on the HSE's official Twitter/X or Facebook pages.

Professional networking:

- Using platforms like LinkedIn to connect with other healthcare professionals and to share knowledge and best practices.
- Example: Sharing articles or research findings relevant to public health on your professional profile.

Public health education:

- Sharing general health information that does not disclose personal patient data.
- Example: Posting tips for healthy living or information about seasonal flu on personal or professional accounts, ensuring no patient information is included.

When it is not appropriate for staff to post on social media

Sharing patient information:

- **Example:** A nurse posts a photo of a patient receiving treatment in a hospital room.
- **Why it's not appropriate:** Under General Data Protection Regulation (GDPR), any information that can identify a patient, directly or indirectly, is considered personal data. Posting images of patients without their consent, can lead to breaches of privacy. It can also violate the GDPR principle of data minimisation, which requires that only necessary data be processed by the HSE.

Inappropriate communication:

- **Example:** A healthcare administrator shares a post on social media about a recent patient success story, including a photo of the patient, HSE hospital location and specific details about the patient's medical condition and treatment plan.
- **Why it's not appropriate:** Sharing identifiable patient information without explicit consent violates GDPR's requirement for lawful processing of personal data. The principle of transparency mandates that patients must be informed about how their data is used. Sharing details on social media, as in the example shown, publicly undermines this principle.

Confidentiality breaches:

- **Example:** A doctor shares a message in a WhatsApp group chat with colleagues that includes images of a patient's injuries and details of medical records.
- **Why it's not appropriate:** GDPR emphasises the importance of confidentiality and security in handling personal data. Using personal messaging apps for sharing sensitive patient information can lead to unauthorised access and data breaches, violating the GDPR's security requirements.

Inappropriate professional disclosures:

- **Example:** A healthcare professional writes a post on social media discussing a challenging case they handled, including identifiable details about the patient's condition and treatment.
- **Why it's not appropriate:** GDPR requires that personal data be processed fairly and in a transparent manner. Discussing identifiable patient cases in public forums without the patient's consent can lead to reputational harm for the patient and is a breach of their right to privacy.

Unauthorised content sharing:

- **Example:** A hospital staff member uploads a video showing their day working in a hospital setting, on the wards, including footage of a patient without their consent.
- **Why it's not appropriate:** GDPR says that personal data must not be processed without the data subject's consent. Sharing videos that include identifiable information without explicit permission is a serious violation of patient rights and can lead to legal repercussions.

Public identification of patients:

- **Example:** A healthcare worker posts about a specific incident involving a patient, mentioning the patient's first name and the nature of their treatment.
- **Why it's not appropriate:** GDPR protects a person's rights to privacy and data protection. By disclosing identifiable information in a public forum like a social media platform, the healthcare worker risks exposing the patient to unwanted attention and potential harm, which is contrary to the principles of data protection.

These examples show the importance of following GDPR principles when using social media in healthcare settings, and emphasise the need for consent, confidentiality, and the responsible handling of personal data.

*Data minimisation is a key principle under GDPR that requires organisations to collect and process only the personal data that is necessary for the specific purpose. This means ensuring that the data collected is adequate, relevant, and limited to what is needed. By adhering to this principle, we reduce the risk of unnecessary data exposure and enhance data protection.

Use of recording devices by service users and visitors in healthcare settings

The use of recording devices, such as smartphones or tablets, by patients and visitors to document their experiences in healthcare settings has become more common. This technology can support communication and documentation, but its use must be carefully managed to protect patient confidentiality and to prevent sharing of recordings on public platforms such as social media.

Permitted and prohibited use of recording devices

To protect the privacy and confidentiality of all patients, visitors, and staff, the use of recording devices (including photo, video, and audio recording devices) is generally prohibited on all HSE hospital property and grounds. Unauthorised recordings may capture other people's personal information without consent.

However, patients are permitted to make audio recordings of their own consultations with clinicians or take photos of their own personal records. Under GDPR, such recordings are considered personal note-taking and are permitted.

Please note: These recordings must be limited strictly to the patient's own interactions with clinicians. Recording others without their consent remains prohibited. For further reading please refer to the HSE Point of Care Access policy.

Patient recordings: benefits and risks

Patients choosing to record their consultations—whether made overtly or covertly—can offer certain benefits, but it also carries some risks:

Benefits

- Allows patients to remember important advice, particularly where there are language barriers.
- Provides a copy of the consultations when patients may have been distressed.
- May help patients and their family members in cases where patients may be experiencing memory loss or have some cognitive impairment.
- Includes patients' family members in their care and decision making.
- Helps patients to remember if the information is particularly hard to understand.

Risks

- May indicate a level of distrust and lack of confidence, negatively impacting ongoing medical care.
- May interfere with the natural flow of conversation.
- Overt recordings of medical encounters may also alter doctor decision-making. A feeling of 'needing to appease' during a recorded consultation may lead to a patient having more invasive or aggressive testing, unnecessary referrals and expense for the patient and healthcare system.
- May risk compromising the confidentiality of other patients or visitors if recordings are not made in a private area.
- With modern artificial intelligence editing tools, it is increasingly common for recordings to be edited and manipulated.

When used responsibly, recordings can be a helpful tool in healthcare—but without caution, they may lead to privacy breaches or other serious consequences.

Guidance for patients when recording consultations

The following guidance is intended to help service users understand how to record their consultations in a respectful, lawful, and responsible manner.

- People's privacy must be respected. People who use our service should record their own care only and should not record anyone without permission, including staff or other patients.
- Recordings should be done openly and honestly. People who use our services should inform the staff they wish to record their conversation and ask for their consent to do so.
- Where a recording is made entirely for personal reasons, it is unlikely to be in breach of GDPR. However, such recordings are strictly for private use and must not be published online, including on social media platforms, or used in any way that could harass or harm others.
- People who use our service should be aware of the private and confidential nature of the recording. It is their own responsibility to keep it safe and secure.
- The misuse of a recording may result in criminal or civil proceedings as a breach of GDPR.

Guidance for frontline staff on managing patient recordings

Frontline staff have a responsibility to help patients to understand the information discussed during their consultations. The following guidance is for frontline staff on how to respond when a patient wishes to record their consultation or treatment.

- Frontline staff should accommodate patients wishing to record their consultation wherever possible and ensure that no other individuals who have not consented appear in the recording.
- Frontline staff should remind patients that recordings must only be used for personal purposes and must not be published in the public domain (e.g., on the internet or social media) or used to harass staff, other service users or hospital visitors.
- If a frontline staff member does not consent to being recorded, they should, where possible, arrange for another colleague to provide the necessary care. If no alternative is available, they should continue to treat the patient but request that the recording does not identify them.
- It may also be helpful to explore the patient's reasons for wanting to record the consultation. Understanding any concerns they may have can build trust and improve communication between the staff member and patient.
- Frontline staff who are uncomfortable with being recorded may use this opportunity to explain their concerns and suggest alternative ways to support the patient's understanding. These may include:
- Speaking more slowly or clearly
- Allowing a friend or relative to be present
- Sending a follow-up letter after the consultation
- Frontline staff should also document the recording and consent arrangements in the consultation notes.

Recommendations for staff in event of staff or service users being recorded without consent

- If a patient or visitor is suspected of recording someone without their consent:
- **Remain calm and professional:** Address the situation in a non-confrontational manner. Politely ask if the person is recording and why. If they say yes, request that they stop recording immediately as they are recording without consent. Ask for the recording to be deleted.
- **Explain policy:** Inform them that recording without consent is not permitted under HSE policy. Highlight that it may breach privacy rights, GDPR, and hospital or service-specific rules.
- **Escalate if necessary:** If the person refuses to stop or becomes confrontational, alert your line manager or hospital security for support.
- Document: Record details of the incident in line with the hospital's reporting procedures. Consider whether it breaches hospital policy or legal standards and if the Data Protection Officer needs to be involved.
- **Provide support:** Offer support to any affected staff or patients, ensuring their concerns are acknowledged and addressed.

Steps to take when encountering social media posts from members of the public

In today's digital age, it is increasingly common for members of the public to record and share their experiences in healthcare settings on social media. This section of the guidance aims to help HSE staff respond appropriately to such situations, ensuring compliance with data protection laws and maintaining patient confidentiality.

1. Assess the situation

- **Identify the Content:** Find out what kind of content is being shared. Is it a video, photo, or comment? Does it include information that could identify a patient or a member of staff?
- **Evaluate the Impact:** Consider the potential implications of the post on patient privacy, staff reputation, and the hospital's image.

2. Document the post

- **Take screenshots:** Capture screenshots of the post, including the date, time, and the account that shared it. This documentation may be necessary for any follow-up actions.
- **Record context:** Note any relevant context surrounding the situation, such as the location, time, and any interactions that occurred prior to the recording.

3. Report the incident

- **Notify management:** Inform your line manager or the designated social media or communications officer in your region within the HSE about the post. Provide them with the documentation you collected.
- **Involve Data Protection Officer:** If the post contains identifiable patient information, complete a data breach incident form including clear details of the incident to help HSE's local Data Protection Office assess potential breaches of GDPR.

4. Engage with the public (if necessary)

- **Do not engage directly or respond on social media:** Avoid commenting on the social media post or engaging online with the individual who shared it. This may escalate the situation or lead to further breaches of confidentiality.
- **Official response:** If deemed necessary, allow the HSE communications and / or Data Protection team to handle any public or direct response. They can provide a professional and consistent message that addresses the situation while protecting patient confidentiality. You will find contact details on hse.ie

5. Educate and inform

- **Raise awareness:** Use this opportunity to educate staff and the public about the importance of patient privacy and confidentiality. Consider sharing information about HSE policies regarding social media use.
- **Promote respectful sharing:** Encourage the public to share their experiences respectfully and responsibly, emphasising the impact of their posts on individuals' privacy.

6. Review and reflect

- **Evaluate policies:** After addressing the situation, review any existing policies and procedures related to social media and patient privacy. Consider whether updates need to be made, or if additional training is needed for staff.
- **Learn from the incident:** Reflect on the incident to identify any lessons learned and improve future responses to similar situations.

Compliance with GDPR and Irish Data Protection Law

To ensure compliance with data protection laws, consider the following:

1. Anonymisation

Always anonymise any data shared on social media, and make sure that no identifiable information is included.

2. Consent

Get clear explicit consent from patients, service users or employees before sharing any information that could identify them on social media, even in a professional HSE-endorsed context (HSE consent form for photography, audio, video).

3. Training

Participate in HSE training programs on data protection and social media use to stay informed about best practices and legal obligations.

4. Reporting breaches

If you suspect a data breach or inappropriate use of social media has taken place, report it immediately to your line manager. If a personal data breach is confirmed by a staff member, you must complete a data breach incident form and send to your local data protection team or the HSE data protection officer DPO@hse.ie (See Appendix B for the HSE Data Breach Incident Reporting form).

Public engagement

Social media is about having two-way conversations, so engaging with others online is a natural practice. When engaging with members of the public on social media, whether in a personal or a professional capacity, please adhere to the following best practice:

- Ensure the person you are engaging with is a real person and not a bot. A bot is an automated account, usually on Twitter/X, which pushes out hundreds of posts without any personal information being shared.
- Always read the biography or 'about' section of a person you are engaging with on social media.
- Review their last 5-10 status updates or Tweets to get a sense of their opinions and views to see if you have shared interests.
- If you are experiencing trolling or offensive, aggressive or threatening behaviour, screenshot the posts as evidence, block the person/s on the social network and report them to the social network.
- If a colleague is subjecting you to cyber bullying, follow the steps in the 'HSE Escalation and Takedown guidelines here and report the matter to HR along with screenshots of the offensive posts/comments.

REMEMBER: How to spot a bot

- **Activity:** Does the account tweet or post hundreds of times per day or per week?
- **Anonymity:** Does the account lack personal information or any identifying information?
- **Amplification:** Does the account mainly re-share content from other accounts and not original content?

Real world examples of inappropriate use of social media

Please find below some real-life examples of inappropriate use of social media in a hospital and healthcare administration setting, focusing on patient and employee privacy, on various social media platforms. These cases resulted in fines, sanctions and or loss of trust in those organisations as well as consequences for those involved.

1. Instagram

Real world example: A healthcare provider in the UK faced backlash when a staff member posted a photo on Instagram of a patient in a vulnerable state during treatment. The post, which included identifiable information, was shared publicly and led to a significant breach of patient privacy, resulting in disciplinary action against the employee.

2. Facebook

Real world example: A hospital in the United States accidentally posted a patient's personal health information on its Facebook page. The post included details about the patient's diagnosis and treatment, which were visible to the public for several hours before being removed. This incident led to a formal complaint to the hospital's data protection officer.

3. WhatsApp

Real world example: A group of healthcare professionals in a hospital used WhatsApp to share images of patients during a medical conference. One of the images included identifiable information about a patient's condition. This breach of confidentiality resulted in an investigation by the hospital and highlighted the risks of using personal messaging apps for sharing sensitive information.

4. LinkedIn

Real world example: A healthcare executive posted a detailed article on LinkedIn discussing a recent case involving a patient. The article included specific information about the patient's medical history and treatment, which led to the patient being identified by others in the LinkedIn community. The healthcare provider faced criticism for failing to protect patient confidentiality.

5. YouTube

Real world example: A medical professional uploaded a video to YouTube showing a surgical procedure. The video accidentally included identifiable information about the patient, such as their name and medical history, in the background. The video was taken down after a complaint was filed, but not before it had been viewed thousands of times, leading to a significant breach of privacy for the patient.

X (formerly Twitter)

Real world example: A healthcare worker shared information online about a patient's treatment, mentioning the patient's first name and specific details about their condition. The post went viral, leading to public identification of the patient. The healthcare provider faced scrutiny for the breach of confidentiality and had to implement stricter social media policies.

These examples show the potential risks and consequences of personal data breaches in healthcare settings when using social media platforms. They also show how important it is for HSE staff to follow privacy guidelines and data protection laws.

Part 3

Social media for personal use

Part 3: Social media for personal use

Everyone has personal preferences about how they use social media. Some people choose to use it frequently; others choose to have accounts for private messaging only.

Personal profiles are in fact, personal. However, the following best practice guidelines should be adhered to, to protect your own personal reputation and that of your employer.

Social media is a fundamental way in which we communicate.

Social media, for the purposes of this guidance, includes any technology that facilitates creation or sharing of any form of content on a virtual platform, such as Facebook, LinkedIn, Twitter, WhatsApp, TikTok, Reddit, Snapchat, YouTube and all other social networking sites. The guidance also includes discussion forums, image sharing platforms (i.e. Instagram, Pinterest) instant messaging applications, internet postings, blogs, etc.

Staff should assume that anything that they do on social media – whether on a professional or personal account – could be viewed by a colleague, supervisor, regulator, patient, or service user. As such, any social media activity, even from your personal account, may have a positive or negative impact on the HSE's reputation. Engagement in social media activities always requires the exercise of due care and sound judgement. It is recommended to take a moment to review and reflect all content, especially if it has any reference to the HSE, our service users or employees, for accuracy, and consider the potential impact of the message before you post, share, comment or like.

- Social media is about connecting, conversing, helping others and sharing.
- Social media is a valuable resource to learn, be entertained, conduct research, promote news and events and to contribute to topical conversations.
- Social media is more than just Facebook, X (Twitter), Instagram, TikTok, Snapchat, YouTube and LinkedIn. It includes blogs, online forums and any other Internet-based tools for sharing and discussing information such as blogs and messaging apps WhatsApp and Facebook messenger.
- Social media content is indexed in search engines, which means that the content you post on public networks is traceable on Google or other search engines.
- Social media is a resource for news, but you should fact-check any news or information that you are sharing. Fake news is a growing trend on social media.

REMEMBER

Data protection laws protect an employer where the employees' use of social networking sites causes damage to that organisation's reputation or leads to the release of confidential information.

Social media etiquette

- Respect others' views and opinions. It is understandable that you may not always agree with opinions online, however, do not engage in a public disagreement.
- Try to add value to what others are doing and saying with your knowledge and insights. Remember you are not the customer-facing voice of the HSE, the HSELive team fulfil this role. However, feel free to signpost to them.
- Act professionally when engaging on social media, particularly if you are engaging in a work capacity.
- Be quick to correct your own mistakes and admit when you are wrong.
- Do not use slurs (e.g. ethnic, religious), insults or obscenities.
- Do not engage in conduct that would be viewed as unacceptable offline.
- Be considerate of others' privacy and topics that could be considered personal, such as religion or politics.
- Do not engage with trolls whose aim is to engage you in negative conversation.
- Share information that you know to be true; be careful of fake news and sharing misinformation.
- Do not share information about friends or colleagues without their prior consent.
- Do not record or take photos of staff or service users without their consent.
- Remarks made in the name of the HSE about individuals, organisations or groups which are of an offensive, derogatory or threatening nature on social media may result in disciplinary, legal or criminal action being taken.
- Speak in the first person, remembering that you are publishing content in your own name and not that of your employer i.e. I not we
- Confidentiality – as per the terms and conditions of your employment you shall not discuss or disclose any information of a confidential nature except in the proper course of your employment.

REMEMBER

You are legally liable for anything you publish on your own social media accounts.

Linking the HSE to your personal social networks

- If you refer to the HSE as your employer in your social media accounts, you should be mindful that you are publicly connecting yourself to your place of work.

- Confidential and proprietary information relating to your work should not be published online, either on public or in private messaging apps.
- Having an opinion on topics in the public domain relating to the HSE is acceptable but be mindful that any opinions or comments should be based on fact.
- Be mindful that your opinions will be monitored by the media who use social media as a research tool. If you are not an official spokesperson for the HSE then you should refrain from expressing professional views in the public domain.
- Public queries relating to HSE services are dealt with by the HSELive team who are highly trained and skilled in dealing with the broad range of questions received on a daily basis.
- If members of the public contact you for an answer to a HSE-related query, you should direct them to the HSELive team, the customer service arm of the organisation.
- Confidentiality: as per the terms and conditions of your employment you shall not discuss or disclose any information of a confidential nature except in the proper course of your employment. Do not record or photograph staff or service users without their consent.

Signposting to HSELive

If you are asked a specific HSE-related question on social media, please signpost the user to the following communications channels.

- **Live Chat**
  Talk to a member of the team live on the HSE website http://www.hse.ie/eng/HSELive

The HSELive team answer questions from members of the public from 8am - 8pm Monday to Friday and from 10am - 5pm on Saturdays.

- **HSE X** (Twitter), Facebook and Instagram

You can send the social media team via a direct message on Twitter, Facebook or Instagram with an average of a 2-hour response time during hours of 7.30am to 9pm Monday to Sunday.

- **Phone Freephone 1800 700 700**
  You can call the HSELive team from 8am - 8pm Monday to Friday and from 10am - 5pm on Saturday.
- **Email** hselive@hse.ie
  Send us an email and your query will be dealt with by the appropriate person/department.

Social media abuse

Nobody is immune to online abuse, but there are steps you can take if you feel you have become a victim of cyber bullying at work.

You should report cyber bullying if:

- content is published online about you that is untrue or defamatory
- personal work information is shared online that identifies you or service users (clients/patients)
- you are subjected to sustained trolling

You can report cyber bullying in the HSE by bringing evidence of your complaint to your line manager. Seek advice from your local communications team also.

The best way to report abusive content or spam on social networks is by using the Report link that appears near the content itself.

Even if you don't have an account, you can still report content directly. Some social networks offer a way for non-users to raise concerns through their Help Centre. If you have a link to the specific post or profile, that can be very helpful in the reporting process.

However, please note that submitting a report does not guarantee that the content will be removed. The decision ultimately rests with Instagram, as they assess whether the content violates their Community Guidelines.

Conclusion

It is important that HSE staff are vigilant and proactive when dealing with service users and visitors using recording devices or, creating or looking at social media posts that involve people who use our service, visitors or staff. By following this guidance, staff can help protect patient confidentiality and HSE staff can engage with the public responsibly while ensuring compliance with data protection laws. Always prioritise patient confidentiality and the integrity of the HSE and ensure compliance with data protection laws.

Consequences of misuse

Non-compliance with this guidance is considered a breach. Any misuse of social media should be reported to the relevant member of staff's line manager and in turn to the Head of HR.

Non-compliance can lead to severe consequences, including:

- Disciplinary action, up to and including dismissal.
- Legal action for breaches of confidentiality or defamation.
- Damage to professional relationships and workplace morale.

Monitoring and implementation

The HSE reserves the right to monitor, intercept and review, without further notice, staff activities using our IT resources and communications systems, including but not limited to, social media postings and activities. This may be done for legitimate professional purposes which include ensuring that expected standards are being met by those using the systems. This may also be done to ensure to detect and investigate any unauthorised use of the systems (including where this is necessary to prevent or detect crime).

Managers have responsibilities to ensure that this guidance is implemented in the workplace. This includes ensuring that their staff members are given the opportunity to read and understand the policy and are aware of the standards of behaviour expected. Managers are not expected to monitor social media use from their staff members but are expected to act when they are made aware of behaviour which falls below the level required.

All staff are responsible for the success of this guidance. Staff should ensure that they read and understand it and follow the requirements that the document has outlined. Finally, staff should make sure that their use of social media involving reference to the HSE does not damage the reputation of the organisation.

Review of policy

This Policy will be reviewed by the Data Protection Office and Digital Team in 36 months.

Queries relating to the policy should be sent to digital@hse.ie.

Mary Deasy, Data Protection Officer
HSE Data Protection Office

Muiriosa Ryan, Social Media and Digital Marketing Manager
HSE Communications

Tara Looney, Head of Digital
HSE Communications

Social Media and Data Protection
Staff Use Policy