Estyn

Arolygiaeth Ei Mawrhydi dros Addysg a Hyfforddiant yng Nghymru
Her Majesty's Inspectorate for Education and Training in Wales

Social media guidance

This document is also available in Welsh.

Information sheet

Information box

For further advice contact: Information Services team

Date of publication: July 2021

Version: 6.0

Version control

Version	Author	Date of issue	Comments
1.0	Phil Sweeney	January 2014	Draft for staff comments (issued in conjunction with redraft of IT Usage Policy)
2.0	Information Governance Group	14 April 2014	Review completed
3.0	Phil Sweeney	March 2015	Updated in line with Civil Service Employee Policy: Additions to: para 1.18 & 4.10 New paras: 1.30, 3.21, & 4.7
4.0	Information Governance Group	February 2017	Policy name changed to 'Personal use of Social Media' Added that you should not identify yourself as working for Estyn **or the civil service** on your personal social media. Clarified our position on asking staff to promote Estyn's messages via their personal social media (Para 1.19).
5.0	Information Governance Group	May 2018	Review before introduction of GDPR.
6.0	Information Governance Group	July 2021	Simplified policy title Updated language to bring in line with our Tone of Voice Updated position on identifying employer on social media Removed repetition throughout Added information about LinkedIn Updated social media case studies Updated FAQs Added 'useful links' appendix

This policy has been agreed by Estyn management and trade unions.

Equality Impact Assessment

A business rationale assessment has been carried out and this policy contributes to Estyn’s strategic objectives and delivery principles.

An equality impact assessment has been carried out and this policy is not deemed to adversely impact on any people on the grounds of age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, sex and sexual orientation or Welsh language.

Contents Page

Introduction

We all use the internet everyday, and social media is often an important feature of our time online. It helps us to stay in touch with our friends and families, preserve memories, and share our experiences with communities around the world. As a government organisation, social media lets us connect with our stakeholders in a more immediate and informal way than any other channel. It lets us communicate in a more efficient and open way and reach our stakeholders in the places they are already using to interact with others.

We encourage you to use social media responsibly. When you're online you should be respectful of others and be clear about who you're representing, whether it's you personally or if you're speaking on behalf of an organisation. Whoever you're representing, you should always remember the Civil Service values: integrity, honesty, objectivity, and impartiality.

Our corporate social media accounts are run by the Communications team. These include Twitter, Facebook, YouTube, LinkedIn and the Estyn blog on our website.

Remember that putting something on social media isn't like having a conversation with a friend in public – your post could end up being seen or shared by countless other people, long after you put it online. **If you wouldn't do it offline, don't do it online #thinkbeforeyoupost**

Social media policy guidance

Who does this guidance apply to?

1.1 This guidance applies to all Estyn employees; in their work or personal time, using work or personal devices. This includes permanent and temporary employees, agency workers, secondees, and staff on loan from other government departments.

What is social media?

1.2 Social media is an online platform where you can share digital content, for example text, pictures and videos. Here are some examples:

- Facebook
- Twitter
- Whatsapp
- Instagram
- YouTube and Vimeo
- Linkedin
- Snapchat
- Blogs
- Wikipedia
- Forums and discussion boards

This includes any messaging services that are integrated into these platforms (e.g. Facebook messenger or Twitter DMs).

Why do we need a policy and guidance?

1.3 We've written this guidance to clarify what is and isn't appropriate for our staff when they use social media; it highlights the key things to remember and clarifies boundaries and potential issues to help our staff to use social media responsibly.

1.4 Social media isn't always private. You might think that you're posting something to a specific audience, but anyone who can see your posts can easily copy and forward them on to others. This is also the case for private messages; it's simple to take a screenshot and share it with anyone. Once you share something online, you lose control of it; it can't be taken back.

1.5 It is important to remember that what you do online may impact on your work, the reputation of the Civil Service, Estyn, our employees, suppliers and other stakeholders, so **think before you post.**

1.6 The Government has published a 'social media playbook' which talks about how the govt digital service use social media. Our policy and guidance supports, clarifies and expands on this guidance and provides a framework for employees to feel empowered to use social media responsibly. Links for further useful guidance on how to use social media appropriately are in Appendix 3 – Useful links.

1.7 All civil servants are bound by the Civil Service Code. The Code sets out our core values of integrity, honesty, objectivity and impartiality. It also describes the standards of behaviour that are expected of us whether we're online or offline, in work or personal time. Posting any content online which is considered to be a breach of the Civil Service Code or Estyn's code of conduct may result in disciplinary action (please see the **Misuse** section of this guidance).

Responsibility

1.8 You should apply the same rules when you interact with people online as you would in public or with your colleagues; for example putting something on a noticeboard at work, talking to your friends or colleagues in a public place, or speaking to a journalist. Remember that using social media can make a post difficult to retract.

1.9 You are responsible for everything you post online whether you use your own name or a pseudonym. This includes anything you choose to share on your own social media which has been made by other people. Make sure you read and follow the Terms of Use or Rules of Engagement for the social media platforms that you use.

1.10 If one of your colleagues or another civil servant makes an inappropriate post, you should report this to your line manager. Take care not to inflame the situation or implicate yourself by getting drawn into an online argument.

Respect

1.11 Show the same respect for others that you would if you were interacting face-to-face. Ask yourself:

- Could your post be understood differently by other people, for example the public, the media or your employer? These might not be your intended audience, but anyone could view what you've posted.
- Could it risk the safety or security of you or others? Think about how the information could be used by someone with a different agenda to yours.
- Could it affect the personal privacy of others? For example, tagging somebody in your post about a work meeting or a night out.
- Is social media the best way of communicating what you are trying to say? Although using social media can be very effective, sometimes a quick chat, a phone call or an email might be more appropriate.
- Could your judgement be temporarily affected? For example, if you're under the influence of alcohol.

1.12 People have different levels of online expertise and not everyone will use social media for the same reasons. For example, some people might not want to interact with their colleagues on social media; this is a personal choice and we should all respect it.

Staying safe online

1.13 When you use social media, in work or in your personal life, remember:

- **Use your common sense** – social media helps us work openly and connect with the citizens we serve, just remember to apply common sense!
- **Adhere to the Civil Service Code** – apply the same standards online as you would offline
- **Doubts** – if in doubt, don't post it
- **Accuracy** – check the accuracy and sensitivity of what you're putting online before you make it live
- **Permanent** – remember once something is posted online, it's very difficult to remove it

1.14 How to stay safe online:

- **Learn the rules** of each social media site before using it. Be mindful that social media sites often update their guidelines, and it is your responsibility to keep up to date.
- **Use strong passwords** to protect your social media accounts from being hacked into and consider changing them regularly.
- **Check your privacy settings**. Using the strongest privacy settings will help you keep your information safer. You should check these settings regularly.
- **Keep your personal information private** For example, do not disclose your date of birth/location/contact details which could make you vulnerable to others including criminals.
- **Be wary of posts that are offering something too good to be true**, trust your instincts if something seems suspicious. If you know something is fraudulent, report it to the social media site. Be alert to scam messages that are designed to trick you into disclosing information that will lead to defrauding you or stealing your identity.
- **Ensure you have up-to-date, reputable security software** on every device you are using to connect to the internet to help you stay safe online.

Representation

1.15 We understand that you are proud of where you work and you may want to include this on your profile, or talk about it with your friends online. Generally, if you have a personal social media page, **you should think carefully before you choose to identify Estyn or the Civil Service as your employer.** If you share who your employer is, your views could be misinterpreted as being representative of Estyn and the Civil Service. You should be aware that even with a disclaimer, people might think that your employer shares your views.

1.16 If you wish to do so on business social media platforms like LinkedIn, then we suggest that you don't include:

- Details of security clearances held.
- Reference to current or former employment in sensitive jobs.

- Contact details, including place of work or home address – this is particularly relevant if the location could imply association with sensitive employment.
- Detailed CVs or career histories offering information such as project names, budgets or overviews.
- Extensive links to other colleagues in sensitive employment or government services.
- Any information that would potentially disclose confidential and/or sensitive information.

1.17 If you find that someone is misrepresenting Estyn, or posting on behalf of the organisation when they're not authorised to do so, please inform your line manager.

1.18 Sometimes staff might want to share our online content through their personal social media channels. Staff can share content without adding any comments, personal views or any indication that Estyn is their employer. Staff should only share Estyn-related content through their personal channels if they feel comfortable doing so.

Professional representation

1.19 If you are authorised to represent Estyn online through our official social media channels e.g. our blog, you should follow the principles described in this guidance. This applies at all times that you are representing Estyn whether through a professional or branded account, on work or personal IT equipment. Make sure that you only share or comment on information that is accurate, complies with our policy, and which you're authorised to share. Information, client contacts and passwords linked with business social media accounts belong to Estyn and remain the property of Estyn even after a person is no longer employed by us.

1.20 The Government Digital Service and Home Office's joint social media guidance has more information on using social media for business.

Access

1.21 Our stance on accessing your social media accounts during work time is included in our IT usage policy. It is your responsibility to make sure that your use of social media doesn't affect your ability to carry out your work with integrity, honesty, objectivity and impartiality.

Misuse

1.22 If you use social media inappropriately (either at work or in your personal time), this could lead to disciplinary action being taken by Estyn. Inappropriate use could include:

- Bullying or harassment. Online bullying and harassment is just as serious as it is in person. It could be using threatening or abusive language, or posting crude jokes or derogatory comments. Everything covered in Estyn's bullying and harassment policy also applies to your interactions online.
- Posting comments which are inconsistent with Estyn's standards and values and/or the Civil Service Code.
- Posting inappropriate material which brings Estyn into disrepute.

- Posting derogatory/defamatory comments about any person or organisation. A defamatory statement is one that gives false information which damages the reputation of another person or organisation. This could include sharing information that has originally been shared by other; when you share something, you can personally be held liable for the content as if you had posted it yourself.
- Disclosing confidential information about Estyn's business, our employees, suppliers or other stakeholders.
- Spreading rumours or reposting inappropriate comments about Estyn, our employees, suppliers or other stakeholders.
- Any use of personal social media during work time which negatively impacts your ability to carry out your work.

1.23 If you see a colleague or another civil servant acting inappropriately online you should inform your line manager. You might want to print or take a screen shot of the content to pass onto your line manager. Try not to get directly involved; you shouldn't add comments to the post or approach the person as it may not be your place to moderate their post. Instead, pass the information to your manager and allow them to deal with it appropriately.

1.24 If you're a manager and a member of staff reports inappropriate use of social media to you, here are some things to consider:

- Make sure you have a full understanding of the type of social media used and what audience it reaches.
- If it's possible, get a screen shot or print out of the post.
- What is the risk to Estyn?
- Does the content affect another employee? For example, if somebody felt that they were being bullied online.
- Do you need to involve anybody else? For example, do you need to tell Estyn's Stakeholder Engagement team, HR team, Information Technology Cyber Security Officer or another member of senior management?
- Is there a need for an in-depth investigation?
- Would it be appropriate to ask the individual to remove the content? You might want to make a note of their response.
- What are the disciplinary options you can take (if any) and are they proportionate with the effects or potential effects of the content?

Remember that each case should be treated individually.

1.25 It is the responsibility of all employees to make sure that their online interactions are within the law, for example defamation, copyright, equality and data protection laws. A legal breach could include publicising confidential information or personal data without consent which breaches the General Data Protection Regulations. If your actions are considered to be criminal then they could lead to prosecution.

1.26 Employees are required to cooperate fully with investigations into any alleged breaches of this policy. This could include providing information about or access to online material, and removing online content when asked to do so.

Monitoring

1.27 We don't routinely monitor personal use of social media. However, in exceptional cases, where we've been made aware of a potential impact on the organisation, our employees, suppliers or other stakeholders, we reserve the right to investigate an employee's social media use both within and outside the workplace.

1.28 Excessive use of social media in the workplace, whether using work or personal devices, can be monitored as part of our IT usage policy.

Appendix 1 – Social media case studies

Positive examples of using social media

Social media helps organisations to:

- engage with employees and customers on a wider scale
- communicate in a more immediate way
- be more transparent and accountable

Here are some examples of when this has worked well.

Example 1

Estyn led a campaign to reduce teachers' workload working with 17 other organisations, including Welsh Government, regional consortia and education unions. Social media was one of the highest drivers sending users to the campaign webpage. Each organisation promoted the messages through their own channels, leading to over 50,000 Twitter impressions through both of our Twitter accounts (@EstynHMI and @EstynAEM). The social media campaign resulted in over 3,000 downloads of the poster and also generated conversation and endorsements from teachers.

Example 2

The Food Standards Agency (FSA) used social media throughout the London 2012 Olympic Games to monitor conversations on social media sites. This allowed them to see what people were talking about and they quickly dispelled rumours of a food-related norovirus outbreak. They could have two-way communications with the public on social media, and share key messages and news with the online community immediately.

Example 3

Wrexham Football Club used social media in their fight to save the football club from extinction. They raised £100,000 in just 24 hours by using social media to communicate and raise awareness across their fan base. Fans shared information between different social media platforms and the support they received secured the future of the club.

Example 4

The Civil Service Fast Stream team created a Facebook page to interact with potential applicants and share information about the Fast Stream programme. Existing Fast Streamers within the Civil Service post information about their job and career, inviting questions from their audience. The answers are visible to everyone, which gives an immediate insight into the work of Fast Streamers within the Civil Service.

Potential risks of using social media

With the increasing popularity of social media, there are more potential instances of bullying, harassment, discrimination, time wasting and inappropriate use of the platform. These case studies show some of the risks and give examples of how they can be mitigated.

Example 1

An employee working in a customer service role posted offensive comments on her Facebook page about several customers who had subjected her to verbal abuse. The employee had identified her place of employment and a complaint was made to her employer by a customer. This resulted in disciplinary action being taken against the employee for bringing the employer’s name into disrepute.

Remember:

- Regardless of your privacy settings, you can’t guarantee that what you post online will stay private.
- If you've identified your employer and the nature of your comments brings them into disrepute, you could be disciplined and even dismissed.

Example 2

An employee posted inappropriate comments about a colleague on Facebook. This employee had set his privacy levels to ‘friends’ only. One of his Facebook friends passed the comments on, and they were sent to the employee’s manager. The comments were regarded as harassment and constituted gross misconduct, resulting in the employee’s dismissal.

Remember:

- Setting your privacy settings to ‘friends only’ doesn’t guarantee that what you post won’t be shared.
- Bullying and harassment is treated as seriously online as it would be offline. Managers should treat any information they are given with the utmost importance and act upon it immediately and appropriately.

Example 3

An employee was upset with his employer and posted negative comments about them on his personal Facebook page. One of the employee’s Facebook friends brought these comments to the attention of the employer and the employee was subsequently dismissed. The employee argued that he had not identified who he worked for and that his Facebook page was private. The dismissal was upheld as fair, as the employer had given all staff a handbook clearly stating how they should present themselves in public and online.

Remember:

- You shouldn't expect privacy on social media, as comments and content can easily be forwarded on to others. Once it has been passed on, the content is out of your control.
- Activities outside of work that affect Estyn's interests and reputation are covered by our policies and guidelines, and breaching them could have serious consequences. You could face disciplinary action and/or dismissal. If your actions are considered to be a criminal offence, it could also lead to prosecution.

The following case studies show the positive impacts that social media can have.

Targeting a new audience on a low budget

Estyn

In spring 2019 we designed the campaign to recruit young people to become part of inspection teams. This was the first time we had directly engaged with college students in this way.

Our target was to recruit 25 student inspectors. We created a suite of eight films using members of Estyn staff to appeal to the 18 to 25-year-old audience. The films were calls to action to apply for the role of Student Inspector.

Working closely with the communications teams in FE colleges we also created posters, social media graphics and application focusing on making the visual materials engaging to make our messages memorable.

The Twitter social media campaign gained 58,249 impressions and had 626 engagements. We boosted the Facebook video posts at a cost of £200 achieving an English language video reach of 25,317 with 2,177 total views and a Welsh language video reach of 25,825 with 2,179 total views.

Creating a new style of branding for the student inspector campaign resulted in inviting 24 students to our training. The more relaxed tone of the films drove engagement with the age group and working with FE colleges helped spread our messages further. The colleges were proactive on social media, and displaying the posters and digital collateral on campus certainly helped the reach of the campaign.

First World War Centenary Commemoration

Department for Digital, Culture, Media and Sport

In October 2012 the Government set out its ambition for a truly national First World War (FWW) centenary commemoration on which to build an enduring educational and cultural legacy.

To meet comms objectives of Understanding, Remembrance and Recognition, DCMS targeted a national audience with a particular focus on young people and mothers of school-aged children.

Creating emotional resonance was crucial in bringing the FWW to life and making it meaningful for 21st century audiences. This meant working with descendants and creating case studies that would engage people across the UK. This was a fully integrated campaign which was digitally-led with bespoke social media content plans for each major event and a steady drumbeat of awareness-raising activity in between.

The campaign achieved some impressive statistics. Social media coverage of the armistice commemorations had 1.2 million mentions and achieved 809 million impressions with engagement in 164 countries around the world. Also, since the start of the campaign, the Imperial War Museum has welcomed over 9 million visitors to its museums. A 21% increase on the previous four years. The campaign helped drive more than 8 million life stories to the IWM 'Live of the First World War' website.

Appendix 2 - Frequently asked questions

If I don't use social media, how does the policy apply to me?

Even if you don't use social media outside work, your colleagues, friends and family are able to share information and pictures of you. If you don't want them to share anything about you on their social media, you should discuss your preferences them. In terms of your work, this policy supports the digital strategies set out in the Civil Service Reform Plan which aims to further develop digital capability throughout the Civil Service.

What about my right to privacy?

Under The European Convention on Human Rights (the Convention), everyone has the right to respect for their private life. This policy respects the right to privacy and seeks to uphold it by encouraging others to value your privacy rights online.

What about my right to freedom of expression?

The Convention also states that everyone has the right to freedom of expression. However, with rights come responsibilities, and your views shouldn't be posted online if they harm the rights or reputations of other people and organisations.

I use social media in my own personal time, so why can my employer discipline me for using it inappropriately?

How you use social media outside working hours is generally of no concern to us, as long as it doesn't adversely affect us, our employees, our suppliers or other stakeholders. Because social media is in the public domain, your employer has the right to investigate anything that has a negative impact on them.

What if I have made a mistake online?

Remove the post or content as soon as you can, but keep in mind that others may have already forwarded or copied it. Be upfront about your mistake and try to rectify it where possible. If the information is about Estyn, our employees, suppliers or other stakeholders, then tell your manager as soon as possible.

What should I do if I think I am being bullied or harassed online?

If you feel able, talk to the person and ask them to stop; this could resolve the situation quickly as they might not realise they're being offensive. If you don't feel able or if this doesn't resolve the situation, refer to the bullying and harassment policy or speak to the HR team for advice. You can also speak to your line manager or a member of the PCS/FDA executive board in confidence. If you can, make a record of the offensive posts or content (for example by taking a screen shot or printing it off).

What if a third party attributes a comment to me on social media that I said to them in private?

It is possible that a third party could attribute statements or opinions to you that you didn’t intend or wouldn’t have posted yourself. If this happens, you should ask the person who made the statement whether they would be willing to remove it, but you shouldn’t press them to do it as this might make the situation worse. It is important that you don’t get involved in any kind of debate with the person involved, and you should try not to make statements to anyone about the post in question. If the comment has links to your job, then you should let your line manager know what has happened.

in general, you should always be careful what you discuss and who you discuss it with:

- Don’t disclose sensitive or confidential information about other people, your work or your workplace as this could breach the Data Protection Act (DPA) or other legislation.
- Don’t defame individuals or organisations (posting untruths).
- Don’t bully, harass or discriminate.
- Don’t break copyright laws.

Appendix 3 – Useful links

- **Get Safe Online -** https://www.getsafeonline.org/
- Unbiased, factual and easy to understand information regarding social media.
- **Digital Unite** - http://digitalunite.com/
- Learning opportunities and support in using online technology (including Facebook, Twitter and blogs).
- **Social media guidance** - https://www.gov.uk/government/publications/social-media-guidance-for-civil-servants/social-media-guidance-for-civil-servants
- **GCS info on propriety on social media** https://gcs.civilservice.gov.uk/guidance/propriety-in-digital-and-social-media/