Polisi Cyfryngau Cymdeithasol
Social Media Policy

sirgar.llyw.cymru
carmarthenshire.gov.wales

Cyngor Sir Gâr
Carmarthenshire
County Council

1.Policy Statement

1.1 This is the Carmarthenshire County Council social media Policy. Carmarthenshire County Council will ensure all employees are aware of what is considered to be acceptable use of social media, both professionally and personally.

2. Purpose and scope

2.1 This policy sets out Carmarthenshire County Council's (the Council's) policy regarding the use of social media for both work-related and personal purposes. It applies to all employees employed by the Council.

2.2 This policy does not relate to Members of The Council who should refer to the Code of Conduct applicable to them.

2.3 Used appropriately and within the prescribed guidelines, social media is a useful way through which the Council can communicate, connect, and engage with the people of Carmarthenshire and wider afield. It is key to the corporate strategy of the Council, to demonstrate the Council's commitment to listen and engage with our communities, partners and all stakeholders to inform our improvement plans.

2.4 This policy aims to provide a guide to help the Council and its employees to avoid problems which arise when social media is not used appropriately, including the risk of disciplinary action, damage to the Council's reputation and/or legal action being taken against the Council. When using social media, it is important that any activities are performed in line with the Council's policies, procedures and guidance listed in point 10.1 of this policy.

2.5 This policy relates to the use of social media across all platforms including but not limited to Facebook, X, Instagram, Threads, Vimeo, Pinterest, TikTok and Umbraco (Newsroom).

3. Standards of behaviour in relation to internet use

3.1 Procedures for the use of the internet by employees using Council-owned equipment and facilities is governed by the Internet Usage and Monitoring Policy Version 2.0, Employees are reminded that this guidance states: -

> *'No employee, consultant or contractor will attempt to access or transmit content that in any way may be interpreted as insulting, disruptive or offensive or which may be harmful to employees' morale. Examples of prohibited material include but are not limited to*:
>
> - *Sexually explicit messages, sexually explicit images, sexually explicit cartoons, sexually explicit jokes or sexually explicit movie files*

- Profanity, obscenity, slander, or libel
- Ethnic, religious, or racial slurs
- Any content that could be construed as harassment or disparagement of others based on their race, colour, nationality, ethnic or national origins, language, disability, religion, age, gender, gender reassignment, sexual orientation, parental status, marital status or political beliefs'

4. Personal use of social media

4.1 Whilst the Council respects the legal rights of all individuals, employees need to be aware that what they do and say outside of work can often compromise their position inside work. It is important to note that other people's perceptions need to be considered when using social media.

4.2 This policy covers the responsibilities of employees both inside and outside of work time. All employees must pay due regard to the standards set out in the policies, procedures and guidance which are listed in full, in point 10.1.

4.3 Social networking sites must not be accessed during working hours for personal use. Employees should note that this includes personal mobile phone and internet enabled products e.g tablets.

4.4 Employees should never publish or disclose on social media any information about the Council which is not already in the public arena. A breach of confidentiality could result in disciplinary and / or legal action being taken against the employee.

4.5 Do not publish or report on conversations that are private or internal to the Council. Do not cite or reference customers, service users, employees, managers, partners, or suppliers. Be mindful that whatever you publish may be in the public arena for a long time and that doing so may result in disciplinary action being taken against you. You must also ensure compliance with the UK General Data Protection Regulation.

4.6 Ensure that your online activities do not interfere with your job, your colleagues or commitments to customers and the public. Your online activities must always adhere to the relevant policies, procedures and guidance listed in point 10.1.

4.7 Employees identified as working for the council must always act reasonably and responsibly and uphold the reputation of Carmarthenshire County Council. Work related issues should not be discussed on social networking sites even when the issue is anonymised. Employees must not use the Council's logo on personal web pages.

4.8 Even when using social media for personal use, relationships with all persons should always be regardful. The Council acknowledges that in smaller communities, the lines can become blurred particularly where the service user is also a friend or acquaintance – in such cases, employees should disclose an interest to their line manager - common sense and discretion should be applied and all employees must

be aware of the provisions of the Employees Code of Conduct in this regard. In all cases, clarity should be sought from your line manager. The 3 guidance in relation to service users is that employees should not befriend service users that they must maintain a professional relationship with or individuals they support. Employees should adhere to the Close Personal Associations guidance.

4.9 Employees using personal social media accounts in a personal capacity should be mindful that they may still be seen as a representative of the Council. Therefore, the Council's Behavioural Standards in the Workplace policy should be always adhered to, which includes consideration about bringing the Council into disrepute. It is recommended that employees carefully consider referring to their employment with the Council in 'about' or 'personal information' sections of their social media pages as this does not provide a clear boundary between professional and personal conduct. It should be noted that statements confirming personal use of the account (for example 'these views are my own and not of my employer') do not have any legal basis.

4.10 It is advisable that employees do not use a personal social media account for work-related activities. In the rare circumstances where this is necessary, the employee should seek advice from the Marketing and Media team and be aware of the Council's existing policies including Behavioural Standards in the Workplace. There should be a clear statement to confirm professional capacity and the account should never be used in a personal capacity or to give personal or political views.

4.11 Using social media to attack or abuse colleagues, customers/the public or suppliers (harassment and "cyber" bullying) will not be tolerated by the Council. Respect the privacy, feelings, reputation, and position of others you work with. Don't upload or tag colleagues in posts which are defamatory, discriminatory, offensive, or sensitive. Complaints of this nature will be dealt with under the Council's policies, e.g Disciplinary, Equality and Diversity and behavioural standards in the workplace guidance.

5. Using social media for work purposes

5.1 Employees should ensure that with any use of social media in their professional capacity that they must have formal authorisation to use social media on behalf of the Council and follow all set protocols. All service areas wishing to use social media to communicate with the public by setting up a corporate social media account must first gain authorisation. This involves completing a business case which is reviewed by the Marketing and Media team who will provide advice and make recommendations before seeking authorisation from the relevant Head of Service. The business case requires that services first make use of the main corporate social media accounts for a minimum three-month period to trial posts and gauge engagement. In some cases, authorisation will not be granted, and alternative options recommended with reference to the Council's Social Media Best Practice Guidelines. The form can be found on the intranet. Once authorisation is obtained, the relevant employee - with assistance from the Marketing and Media team - must ensure all social media

applications are consistent with the required policies. All new social media accounts must be registered with the corporate marketing and media team and a charge for a social media management licence will be the responsibility of your department. All corporate social media accounts are subject to six-monthly audits based on a sample of 10 accounts.

5.2 Social media accounts set up for work purposes must be appropriate to the business activity and should be clearly marked as a business page, i.e., a business page on Facebook, not a personal page. This could potentially breach articles 7 and 8 of the Data Protection Act 2018.

5.3 The Marketing and Media team carries out a social media audit every six months on a sample of 10 accounts. The audit will identify areas of non-compliance with this policy and the best practice guidelines. The Marketing and Media team has the authority to close, or request the closure, of poorly performing accounts or accounts that do not comply with policy or best practice. Failure to heed a request to close an account will be referred to the relevant Head of Service/Director.

5.4 The Marketing and Media team must be provided with passwords of all corporate social media accounts, and these must not be changed by employees. Passwords will be stored in a secure password management system maintained by the Marketing and Media team and regularly changed and updated to ensure compliance with the Council's password management guidance (http://intranet/our-people/it-support/manage-your-password/). This will be reviewed as part of the six-month audit.

5.5 The Marketing and Media team must be provided with details of all employees with administrative rights. Service areas in control of social media accounts must not add new administrators without first contacting the Marketing and Media team. All new administrators will need authorisation from the relevant Head of Service and given to Marketing and Media to add them on to the corporate business manager.

5.6 All administrators must receive social media training and have a licence to use the Council's preferred social media management platform (which is currently Orlo). All administrators need to be aware that all social media activity is audited with a full audit trail including record of deleted content and comments. Administrative rights may be removed at any time.

5.7 The Marketing and Media team should be notified when an administrator leaves the employment of the Council or changes roles. All access to the administrator's Council's social media accounts will be terminated and passwords will be updated.

5.8 Any unauthorised social media accounts, pages, or administrators identified will be reported to Corporate Management Team (CMT) for consideration. This may result in disciplinary action.

5.9 All social media activity, including content management, monitoring and engagement with members of the public, must be conducted through the approved and audited social media management platform that the Council is in contract with (Orlo). This is to ensure audit compliance. The only exception is where, due to API restrictions, certain functions (for example, event listings, sharing partners posts and sponsored posts) can only be conducted on the native platform. This will be referenced in the audit record for each account.

5.10 All Facebook pages must be linked to the Council's Facebook Business Manager account.

5.11 Corporate social media accounts should not be accessed on personal devices without authorisation from a Head of Service.

5.12 Any proposed use of unsupported or genre based social media will be considered subject to reviewing the security and suitability of the proposed service.

5.13 You must ensure that all communications are compliant with the Welsh Language Standards (No.1) Regulations 2015 that are applicable to all Council employees and communications made on the Council's behalf. All communications must be bilingual. In order to safeguard you and your department it is important that you note that any failure to adhere to the standards set out in the regulations can result in a substantial fine of up to £5,000 which in the event of a breach will be the responsibility of the department from which the breach originates. The necessary guidelines and training on the standards of practice necessary to be compliant with the regulations will be supplied by the Marketing and Media Team.

5.14 All content, including text, images, videos or gifs, must be free from copyright or royalty restrictions. Failure to carry out necessary checks may result in a third party initiating legal proceedings against the Council.

5.15 All of the information, data and communications held on social media platforms and services in the name of the Council is subject to the Breaches of Security policy, which sets out the duties owed under the Data Protection Act and General Data Protection Regulations (GDPR). There is a duty to report any inadvertent / accidental disclosure of information in respect of the Act.

5.16 All content that is published to social media pages is the responsibility of the admin(s) managing the page. If any misuse or signs of profanity is picked up on the page, this matter will be raised with the relevant Head of Service and could lead to disciplinary action.

5.17 Consideration should be given to the pages that you follow and like on social media channels. Consider their relevance to your page and the work that you do. Accounts that are seen to be following inappropriate accounts will be raised in 6 month audit and will be the responsibility of the admin and department to justify the activity to their Head of Service/Director.

6. Monitoring social media

6.1 If a social media account is to be used to view or monitor another account, care must be taken to avoid inadvertently conducting covert online surveillance which is covered by the Council's Covert Surveillance Policy. Advice should be sought from Legal Services.

7. Ensuring adequate safeguarding measures are in place

7.1 Current corporate safeguarding policies apply to any activity on social media and should be always adhered to.

7.2 You must not access any information pertaining to a vulnerable adult or minor under the age of 18, unless expressly required to do so as part of your role (in which circumstances you will have a DBS check). If you are in any doubt, you should discuss any concerns or queries with your line manager.

8. Retaining professional integrity

8.1 For the Council's protection as well as your own always be mindful that it is important that you stay within the legal framework and be aware that libel, defamation, copyright, and data protection laws apply.

8.2 Privacy settings are frequently changed by social media providers and so you need to be aware of any changes to the settings which relax privacy.

8.3 Don't assume your information will be kept private.

8.4 Don't forget that social media tools are owned by external companies and data breaches are possible.

8.5 If in doubt, hold back and seek advice from the Marketing and Media Team. Always consider the content carefully and also be sensible about disclosing personal details about yourself as an employee of the Council.

8.6 When using social media tools to interact with any person in a professional capacity do not treat the tool as a confidential space for confidential or personal conversations. Always assume that anything you share on such tools are in the public domain given that such sites are often subject to attack and data theft from hackers.

8.7 The use of work e-mail to log in to social media should be cleared along with the business case for setting up social media accounts. When using a Council e-mail address (@Carmarthenshire.gov.uk) as a login for a Council social media account, never use your current network password along with it as this creates significant

security risks. Employees must not use their work e-mail for a personal social media account.

8.8 When using social media on behalf of the Council you must act in accordance with the standards set out in the officer's code of conduct in relation to political neutrality (Part 5.4 – Paras 5.0-5.4).

8.9 You must obtain permission from parents / guardians of children and young people under 18 before using their pictures online.

8.10 If you are publishing pictures of people, quoting people, naming employees or members you must make them aware that you are doing so and you must obtain the consent of people pictured, named or quoted. You must obtain express consent to share personal information, including pictures of individuals, and clearly set out where, how, and why their information will be shared. If you decide to use this personal information or picture for any other reason, you must obtain new consent. They must be made aware that they can withdraw this consent at any time and their information or picture deleted immediately.

8.11 You must ensure that your social media accounts are branded correctly and show their connection with the authority. This can be done in the about section of your pages.

9. Monitor and respond

9.1 Whilst social media can be used to broadcast information it is also a communication exchange and when creating public spaces, it is important to monitor what people are sharing or placing on spaces controlled by the Council, the nature of social media carries with it the inherent risk associated with feedback / criticism in the public arena.

9.2 It is the service area's responsibility to manage their social media accounts. Daily monitoring is advised to ensure all comments and direct messages are responded to in a timely manner. Comments posted by persons using any public forum which breach the Council's Social Media Guidance document must be removed.

9.3 You should advise any persons communicating with the Council via social media that any comments they make are subject to the core values of the Council, noted within the Council's Social Media Guidance document, and that any comment which breaches these values will be removed. This must be clearly visible in the 'about' section of each social media page.

9.4 If it becomes necessary to remove offensive, defamatory or libelous comments from other users, inform the Marketing and Media Team. You should inform the user who

made the comments of the reason for the removal after consultation with the Marketing and Media Team and legal services.

9.5 Should any comments be of a criminal nature they, and the identity insofar as it is known, should also be reported to the appropriate authorities.

9.6 Orlo's profanity filter is regularly updated to remove any comments that breach our core values. If you think there are words missing from the filter you think are necessary to add, please contact the Marketing and Media team.

9.7 Any comments that are posted under your posts that are irrelevant to the topic in question can be hidden or deleted on the grounds of the house rules.

10. Related policies

10.1 In considering this policy, please refer to all the policies, legislation and guidance relating to the management of data and information.

- Internet Usage and Monitoring Policy Version 2.0
- Social Media Best Practice Guidelines
- Part 5.4 – Officers Code of Conduct (Revised 14.06.2012)
- Information Security Policy v4.1
- Data Protection article 7 and 8.
- Behavioural Standards in the Workplace Guidance
- Equality and Diversity
- Covert Surveillance Policy
- Customer Complaints and Complaints Procedure
- Welsh Language Standards (No.1) Regulations 2015
- Close Personal Associations/ Relationships at Work Guidance
- Breaches of Security Policy
- UK General Data Protection Regulation