APPENDIX 2

CYNGOR SIR CEREDIGION
CEREDIGION COUNTY COUNCIL

Social Media Policy
for the purposes of the REGULATION OF INVESTIGATORY POWERS ACT 2000 ('RIPA')

22/07//21
Overview and Co-ordinating Committee: 15/9/2021

This Social Media Policy for the purposes of the REGULATION OF INVESTIGATORY POWERS ACT 2000 ('RIPA') ('RIPA Social Media Policy') applies to all Ceredigion County Council ('the Council') employees ('Officers'), including agents of the Council.

It and sets out the position of the Council') regarding the use of the internet, including mobile web browsing, and, in particular, social media websites, when undertaking investigations under and in accordance with RIPA.

Scope

1. The Council recognises the benefits and opportunities that multimedia, such as the internet, provide to access and share information, including a wide range of on-line facilities.

2. This RIPA Social Media Policy should be read in conjunction with the relevant legislation, codes of practice, policies and guidance listed at Schedule 1 below.

Surveillance and Council Social Media

3. Covert surveillance
   Social Media platforms, such as:
   On-line accounts, pages, noticeboards, profiles or other Social Media (such as Council Facebook pages/profiles, Twitter feeds or LinkedIn profiles/pages) owned or controlled by the Council, or private accounts of Officers must not be used for any covert surveillance or investigation without prior consideration being given as to whether a RIPA authorisation is required.

4. Overt surveillance
   Overt use of Social Media (whether inside or outside the scope of RIPA), does not require a RIPA authorisation.

5. These requirements are in place because of the need to:
   - protect the reputation of the Council;
   - to avoid potential consequences of the misuse of Council Social Media; and
   - to ensure compliance with RIPA legislation and guidance.

6. This Policy does not replace the Council's Corporate Social Media Policy (2016), which all Officers using social media sites must also adhere to.

7. This Policy applies when Officers undertake covert surveillance on-line/on Social Media (whether the covert surveillance is RIPA Surveillance or non-RIPA Surveillance (see the Council's Regulation of Investigatory Powers Act 2000 ('RIPA') PART II Directed Surveillance, Covert Human Intelligence Sources and Communications Data Corporate Policy & Procedures Document ('RIPA Policy')).

8. Whilst the use of Social Media to investigate is not automatically considered covert surveillance or activity, its use when conducting investigations/surveillance can mean that it crosses over into the realms of covert and/or targeted surveillance, and become '*misuse*', even if inadvertently done.

9. It is crucial that the provisions of RIPA, as it relates to covert and directed surveillance, are followed at all times when using Social Media in investigations.

10. Advice should be taken from the Corporate Lead Officer-Legal & Governance (Monitoring Officer & Senior Responsible Officer for RIPA) and/or CLO-People & Organisation, should any social media surveillance when using Social Media involve investigating the activities of an Employee of the Council.

11. See the Council's RIPA Policy for an explanation as to what constitutes '*Surveillance*' and '*Private Information*', and which details how there could be an expectation of privacy on-line, and in particular, for information on social media, despite privacy settings.

What is 'Social Media'?

12. This RIPA Social Media Policy will apply to all forms of Social Media/Networking Sites, which are internet based and often includes the construction of a public or semi-public profile. Additional characteristics could include (but are not limited to):

    12.1 The ability to show/share a list of other users with whom the user share a connection (e.g. referred to as '*friends*' or '*followers*');
    12.2 The ability to view and browse the profile's list of connections and that of other users;
    12.3 Hosting capabilities allowing users to post media content viewable by other users; and
    12.4 Community based online social pages, such as discussions forums or chatrooms.

13. Social Media examples include, but are not limited to (as Social Media is a constantly changing area) those listed below:
    13.1 Personal blogs;
    13.2 Posts or comments on any other blogs;
    13.3 Online forums;
    13.4 Online noticeboards;
    13.5 Facebook (social networking);
    13.6 Twitter (microblog);
    13.7 YouTube (video sharing);
    13.8 Flickr (image sharing);
    13.9 Tumblr (blogging/social networking);
    13.10 LinkedIn (professional network);
    13.11 Reddit (forums); and
    13.12 Instagram (image sharing).

Covert surveillance on Social Media & On-line Personas

15. See the Council's RIPA Policy for an explanation of '*covert surveillance*'.

16. The fact that on-line investigation is now routine and easy to access does not reduce the need for authorisation. Investigating and Authorised Officers must understand how the Social Media being used works, since the services provided are not all the same.

17. Officers intending to use covert Council or personal accounts (such as Facebook), to access private postings of individual members of the public/service users, must consider obtaining a RIPA authorisation but note that there is currently no mechanism for a Council Service to operate covert accounts on Facebook within Facebook's

terms and conditions, so any evidence obtained outside of the Site's terms and conditions may breach these terms.

18. Officers must be aware that:

    18.1 unauthorised access to computer material (entering a computer system without permission i.e. hacking);

    18.2 unauthorised access to computer materials with intent to commit a further crime (entering a computer system to steal data or destroy a device or network (e.g. planting a virus));

    18.3 unauthorised modification of data (modifying or deleting data, including the introduction of malware or spyware onto a computer (electronic vandalism and theft of information)); and

    18.4 Making, supplying or obtaining anything that can be used in computer misuse offences

    is a breach of the Computer Misuse Act 1990, which is a criminal offence leading to fines and imprisonment. Examples of breaches could include using a social media site outside of that site's terms and conditions.

19. The Council's RIPA Policy and the Revised Covert Surveillance and Property Interference Code of Practice 2018 at Paragraphs 3.10, and 3.11-3.17 gives further information on when a RIPA authorisation may be needed for online covert activity, and Paragraph 4.16 gives guidance on where previous consent was given.

20. Where on-line personas are permitted to be used corporately, the SRO will maintain a central register of these pseudonyms, profiles/accounts, together with details of the services or individual officers permitted to use/sanction their use.

21. Monitoring will be undertaken by the SRO every 4 months of any usage relating to covert-surveillance on social media and on-line personas, and a list maintained of data/information retained, when that surveillance is likely to obtain a person's private information (whether the covert surveillance is RIPA surveillance or non-RIPA surveillance). This information will be provided by a Designated Officer in the relevant Service.

22. The Designated Officer will provide the information/data to the SRO on a 4 monthly basis. The SRO will also record details of which Services or Officers can use covert-surveillance on social media and on-line personas,/and also which officers can sanction their use.

23. If an Officer wishes to set up an on-line persona for a covert purpose, when private information is likely to be obtained (to include a false identity or false profile) this must only be done with the authorisation the relevant Corporate Lead Officer.

24. Using photographs of other persons without their permission to support the on-line persona, infringes other laws.

25. AOs must also inform the SRO of an Officer's request to set up an on-line persona, providing details of the Officer' authorisation to access the account.

Privacy settings

26. A reasonable expectation of privacy can exist for material published online, if access controls are applied or in in private communication format, such as instant messages. Where privacy settings are available but not applied, the data may be considered open source and, although an authorisation is not usually required, it must be considered. **Repeat viewing of '*open source*' sites may constitute directed surveillance on a case-by-case basis, and the type of the social media is relevant.**

Example1
'Facebook' -if the data is communicated only to 'Friends', it may reasonably be regarded as private information, with an expectation of privacy, as the information is only communicated to an exclusive group.

Example 2
'Twitter'-this may be regarded as communication to the world at large, although where search criteria are entered, it may become directed surveillance.

27. If any member of the public can access the information (e.g. where there is no veto mechanism), it is not private information. Open source information does not usually require authorisation. However, if a profile is built up of an individuals' lifestyle, it may become Directed Surveillance.

28. If it is considered necessary and proportionate for the Council to covertly access sites, which are subject to privacy settings, this can only be done through an appropriate authorisation.

29. Where an Officer intends to engage with others online without disclosing their identity, a CHIS authorisation may be needed (i.e. the activity is more than mere reading of the site's content) e.g. an Officer covertly sends a 'friend' request on Facebook.

30. If a relationship is established or maintained (i.e. the activity is more than a mere reading of the site' content) a CHIS authorisation is necessary:

'*CHIS authorisation is only required for the use of an internet trading organisation such as eBay when a covert relationship is likely to be formed. The use of disguised purchaser details in a simple, overt, electronic purchase does not require a CHIS authorisation, because no relationship is usually established at that stage*.'
(Office of the Surveillance Commissioners 'OSC' Procedures and Guidance 2016 (at 239)).

31. The Officer should consider the purpose of looking at, or attempting to look at, the Social Media information (see the Council's RIPA Policy and revised Covert Surveillance and Property Interference Code of Practice at 3.33).

32. Officers must not adopt the identity (i.e. false profiles/false identity) of a person known/likely to be known to the subject of interest or users of the site without authorisation, and without the consent of the person whose identity is used, and without considering the protection of that person. The consent must be explicit (i.e. the person from whom consent is sought must agree (preferably in writing) what is and is not to be done).

Surveillance Procedures

33. There are three available surveillance procedures that Officers must consider before undertaking surveillance involving SNS/Social Media (see the Council's RIPA Policy for further information, RIPA and the Investigatory Powers Act 2016). They are:

    - The use of **'*Directed Surveillance'***;
    - The use of **CHIS**; and
    - Powers to acquire or obtain '***Communications Data'***.

34. Key issues Officers need to consider include:
    - 34.1 What expectation of privacy a user may reasonably have when posting on the Internet;
    - 34.2 How covert or overt the Officer looking at information on the internet is being; and
    - 34.3 Whether or not a RIPA or CHIS authorisation should be obtained.

<u>Example Scenarios</u>

35. **Scenario 1 – Viewing publically available postings/websites where the person viewing does not have to register a profile, answer a question, or enter any significant correspondence in order to view e.g. a typical trader's website.**

    - There should be a low expectation of privacy and no RIPA authorisation would normally be required to view or record these pages.

    - Nonetheless, repeated visits over time (perceived monitoring) may require a RIPA authorisation. Private information can remain private, even if posted on such a website and the ECHR has construed that the way a business is run *can* be private information. If an Officer intends to monitor in this way, they may acquire private information and this should be done in a systematic way, with results recorded (including whether the Officer happens to access private information). The fact that, on previous visits, a lack of private information is found, could evidence that any subsequent acquisition was incidental and a RIPA authorisation is not required.

    - If a test purchase is required, a fictitious name and address may be used without triggering the need for a CHIS (or Directed Surveillance) authorisation, provided no '*relationship*' is formed. Consideration is needed of the likelihood of acquisition of private information, or how far a '*relationship*' is formed.

36. **Scenario 2 – Viewing postings on social media, such as a social network where the viewer has had to register a profile but there is no other restriction on access e.g. Facebook where there is no need to be accepted as a '*friend*' to view e.g. a Trader has a Facebook '*shop window'* advertising their business/wares.**

    - The person running the site/posting information may reasonably expect viewers to work within the terms and conditions of the website.

    - Viewing should usually, consequently, be done in an overt way i.e. via an account profile using the Officer's correct name, and email address (which should be a Ceredigion.gov.uk email address) or an appropriate Officer set and sanctioned profile. If so, a recording of the visit being made could be presented evidentially.

- If the post/web page does not include private information, a viewing would not engage privacy issues and therefore a RIPA authorisation is not needed. However a mixture of private and business material could be viewable, and, as above, the ECHR construes the way a business is run as being private information. Repeat visits over time so that monitoring could be perceived, may require an authorisation.

- A '*Covert*' account at this level should only be used in the context of a RIPA authorisation.

37. **Scenario 3 – Viewing postings on social networks which require a '*friend*' or similar status to view.**

- Viewings are very likely to include private information, so repeated viewings will constitute '*surveillance*' under RIPA, and so require a RIPA authorisation, which could be whether or not a '*covert*' or '*overt*' account is used (although likely best obtained through a CHIS authorisation, using a covert profile and appropriate risk assessments).

- An '*overt*' account which gains '*friend*' or similar status **may still require a RIPA authorisation**, since it may be that such a status could be granted by default on the part of the person posting/web-page owner.

- The Officer must ensure that their access is being authorised by the relevant Authorising Officer.

- E.g. under Facebook's terms and conditions, only people who know the person who maintains a profile should send to that profile a '*friend*' request. If accepted, that person may mistakenly believe the person requesting is an acquaintance of theirs e.g. they do not recall or know by another name. These persons still have a justifiable expectation of privacy. Since requesting access may not comply with a narrow interpretation of Facebook's terms and conditions, a clearly identifiable **Council Service Sanctioned profile** would then deal with that expectation of privacy, rather than a more neutral Officer based social media profile, such as a Facebook profile with their name, Officer status and details of their employment by the Council, where these details may not be appreciated by the person accepting the '*friend*' request.

- An appropriate Officer set and sanctioned profile must be authorised by the SRO in order to obtain intelligence and provide advice.

Recording Information, Data Handling and Retention Safeguards

38. All data obtained should be appropriately recorded on the relevant form and the Central Register updated. A copy of the submitted form must be retained by the Officer and the original document(s) submitted to the SRO (for updating the Central Register). Part 4of the Council's RIPA Policy sets out the procedures regarding assurance of data handling and retention safeguards.

39. Particular care must be taken regarding sensitive obtained through on-line personas Any information retained must be retained in line with the Data Protection Act 2018, the Freedom of Information Act 2000, and any other legal requirements, including those of confidentiality, and the Council's policies and procedures. Advice can be sought from the Data Protection Officer.

Schedule 1- Relevant Legislation, Codes of Practice, Policies & Guidance

1. This RIPA Social Media Policy should be read in conjunction with all current and relevant legislation, guidance and codes of practice, including (but not limited to) the following:

1.1 The Council's RIPA Policy;
https://ceri.ceredigion.gov.uk/net/wp-content/uploads/2018/05/1.1-S-RIPA-procedure-policy-English-amended-05.10.2017.pdf

1.2 Regulation of Investigatory Powers Act 2000 ('RIPA');
https://www.legislation.gov.uk/ukpga/2000/23/contents

1.3 RIPA Explanatory Notes;
http://www.legislation.gov.uk/ukpga/2000/23/notes/contents

1.4 Documents and guidance issued by the Investigatory Powers Commissioner's Officer ('IPCO') (formerly the Office of Surveillance Commissioner ('OSC') (available at:
https://www.ipco.org.uk/) including OSC Procedures and Guidance Document:
https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/OSC-PROCEDURES-AND-GUIDANCE.pdf

1.5 RIPA Statutory Codes of Practice:

1.5.1 Covert Surveillance and Property Interference Revised Code of Practice 2018;
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742041/201800802_CSPI_code.pdf

1.5.2 Covert Human Intelligence Sources Revised Code of Practice;
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742042/20180802_CHIS_code_.pdf

1.5.3 Bulk Acquisition of Communications Data Code of Practice:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf

1.5.4 Equipment Interference Code of Practice;
(https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/496069/53693_CoP_Equipment_Interference_Accessible.pdf

1.5.5 Communications Data Code of Practice 2018:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/822817/Communications_Data_Code_of_Practice.pdf

1.5.6 Investigation of Protected Electronic Information Revised Code of Practice;
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742064/RIPA_Part_III_Code_of_Practice.pdf

1.6 Home Office Surveillance Camera Code of Practice (2013)
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/282774/SurveillanceCameraCodePractice.pdf

1.7 Investigatory Powers Act 2016 ('IPA');
https://www.legislation.gov.uk/ukpga/2016/25/contents

1.8 SI 2010 N0.521 - Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010; and

http://www.legislation.gov.uk/uksi/2010/521/contents/made

1.9 SI 2012 No.1500 (The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012). http://www.legislation.gov.uk/uksi/2012/1500/contents/made

1.10 The Council's Social Media Policy: https://ceri.ceredigion.gov.uk/portal/employee-handbook/policies-procedures/social-media-policy/

1.11 The Council's Information Security Policy; https://www.ceredigion.gov.uk/your-council/strategies-plans-policies/information-security-policy/

1.12 The Council's Code of Conduct for Local Government Employees*

1.13 The Council's Data Protection and GDPR Policy**

1.14 The Council's Email Policy*

1.15 The Council's Information and Records Management Policy (available at https://www.ceredigion.gov.uk/your-council/strategies-plans-policies/information-and-records-management-policy/)**

1.16 The Council's Policy and Guidelines for Safeguarding Children & Adults at Risk*

1.17 The Council's Social Media Editorial and Administration Policy*

1.18 The Council's Whistleblowing Policy*

*: available on the Council's intranet site (CeriNet)
**: available on the Council's website and CeriNet