Social Media Policy

Scope of this chapter

The increasing use of social media platforms, whether personal or professional in nature, highlight important considerations around our responsibilities towards data protection and how we portray our organisations and professions. It is important to act in a way that does not compromise the confidentiality of clients, the safety and security of staff and their families, or damage working relationships. The use of social media in a social care and safeguarding environment is a developing area. Various reviews have discussed the use of social media in social work practice. There is currently no specific government guidance on the issue for Local Authorities, however, there is guidance from the Regulation of Investigatory Powers Act 2000 (legislation.gov.uk) (RIPA)(see section 2.6 below) and Professional standards - Social Work England. This is supplemented by Social media: protecting what you publish - NCSC.GOV.UK and Social media playbook - GOV.UK (www.gov.uk) In these two latter links, please refer to the security sections.

This chapter is designed to highlight some of the issues to be considered, with links to additional information. It is not intended to provide any legal advice, and legal advice must be sought as appropriate. This chapter will address:

1. The use of social media by staff in a personal capacity
2. The use of social media by staff in a professional capacity
3. Communicating with service users via social media (i.e., WhatsApp)

This chapter will continue to be updated as the body of case-law develops.

Working from Home/Remote Working

It is important to remember that principles of data protection and confidentiality apply equally when working in a home environment as they do when working in an office environment.

Remember that you are still working, and appropriate standards of professionalism should be maintained at all times. Do not post anything on personal social media accounts that could inadvertently disclose any confidential work material/issues/identifying information in relation to service-users.

Introduction

Developments in online facilities such as social media sites are fast-changing. This can impact on many aspects of daily life, including in a social care and safeguarding environment. It is important that professionals keep up to date with and harness useful technology, whilst ensuring that this is done in a safe and appropriate manner.

Social Work England Professional Standard 3.10 provides that social workers will: *'Establish and maintain skills in information and communication technology and adapt practice to new ways of working, as appropriate'.*(Professional standards - Social Work England)

Social media can be a useful tool. It can be used by professionals to develop skills and knowledge, and to network with others nationally and internationally. It offers new ways of working. For example:

- Checking the social media accounts of missing children/young people, where they are public, as part of efforts to trace them;
- Tracing/serving birth parents during court proceedings;
- As part of assessments, to ascertain the veracity of information provided by parents and others.

Local Authority court applications reviewed by the courts and national/ local child safeguarding practice reviews have advocated the use of social media checks during assessments and court proceedings when this has been ordered by the court and there is a clear court direction to support such checks. However, this is a developing area and caution must be exercised.

1. The use of social media by staff in a personal capacity

1.1 Social Work England Professional Standards (Standard 5.6)

This states that a social worker should not *'Use technology, social media or other forms of electronic communication unlawfully, unethically, or in a way that brings the profession into disrepute'*.

In the regulator's **Professional Standards Guidance** on this standard, the following is also stated specifically in relation to social media:

'Confidentiality also applies to the use of technology and social media. Social workers should not make reference to anyone they support or disclose personal or professional information about colleagues, managers, or employers on social media, an online forum or blog. Even if the references are anonymised, the identity of the person may be recognisable to others.

Social media can be a supportive tool to facilitate communication in an online community. However, social networking sites such as Facebook, Twitter, blogs and others are public places.

When communicating online people often have little control over who sees comments or where they end up, even if they are later deleted. Social workers should be cautious about posting information about themselves on social media if it is something that they would prefer the people they work with did not know about.

They should refrain from posting anything that may damage confidence in their work, or the work of the profession. This may include political, religious, or moral beliefs, social activities or personal relationships.

Social workers should also be mindful of their organisation's policies and should not post anything that breaches their employer's code of conduct. At all times, they should uphold the confidentiality of the people they support, as well as their colleagues and the people their colleagues' support.

It is important to apply stringent privacy settings and review them regularly. Privacy settings can be reset by the social networking site to a default which may not be as stringent as personal settings, so it is important to check these regularly.'

It should be noted that inappropriate social media postings from personal accounts have in the past led to Health and Care Professions Council (HCPC) proceedings against professionals.

The HCPC have also previously set out the following *Top Tips* for professionals using social media in a personal capacity, which remain a useful reference point:

- **Think before you post**. Assume that what you post could be shared and read by anyone;
- **Think about who can see what you share and manage your privacy settings accordingly**. Remember that privacy settings cannot guarantee that something you post will not be publicly visible;
- **Maintain appropriate professional boundaries** if you communicate with colleagues, service users or carers. It is not appropriate to 'accept' service users and their carers as online 'friends' in a personal network, as it creates a personal relationship outside of the workplace;
- **Do not post information which could identify a service user unless you have their permission**;
- **Do not post inappropriate or offensive material**. Use your professional judgement in deciding whether to post or share something;
- **If you are employed, follow your employer's social media policy**;
- **When in doubt, get advice**;

IF YOU THINK SOMETHING COULD BE INAPPROPRIATE OR OFFENSIVE, DO NOT POST IT.

1.2 Hertfordshire County Council (HCC) Policy on social media

This section applies whether you are interacting online using an HCC or a personal (non-HCC) social media account, including Yammer.

What you must do:

1. **Always** comply with the HCC Code of Conduct and ensure you do not put yourself in a position where your business duties and private interests/activities conflict.
2. **Always** comply with Social Media Usage Code of Conduct.docx - Herts CC (interactgo.com) and Appendix C - HCC Social Media Policy 2024 [PDF] - Herts CC (interactgo.com) .
3. **Ensure** that business related information posted is true and accurate.
4. **Ensure** that information posted externally is relevant and appropriate to the County Council's remit and represents the views of HCC and not the personal views of any individual.
5. **Ensure** that all business-related information and images you wish to publish are not in breach of legislation or HCC policies.
6. **Ensure** you close the internet when not actively using it.

What you must not do:

1. **Don't** register an HCC business related profile on social media without approval from corporate.communications@hertfordshire.gov.uk.
2. **Never** deliberately access any social media sites that contain or could appear to contain inappropriate content that might cause offence or distress to others when using HCC ICT or premises.
3. **Don't** post/publish personal content or include any links to personal accounts on HCC accounts.
4. **Don't** post/publish any content relating to HCC's activities, workforce or individuals that contains inappropriate material.
5. **Never** post/publish any restricted information relating to HCC's activities or workforce.
6. **Never** undertake any activity which could:

    - Harm or compromise the availability and security of HCC systems.
    - Cause actual or potential damage to HCC's business activities, or
    - Undermine public or business confidence in the Council, its employees, service providers or suppliers.

7. **Never** use, or encourage others to use, social media in any way to attack or abuse HCC, members of HCC's workforce, its suppliers, or members of the public.
8. **Don't** put yourself in a position where HCC would consider that your business duties and personal activities conflict.
9. **Never** upload service user information to Yammer.

For further information, please see the Using digital and social media guide - Herts CC (hertfordshire.gov.uk) and HCC Social Media Policy

2. Use of Social Media by Staff in a Professional Capacity

2.1 Information-gathering during Assessments

Searches of the social media activity of service users and their associates can offer a useful means of information-gathering as part of the Assessment process.

For example, it can be used to check some aspects of a service user's and/or their family's/associate's account of current or recent events which might affect the safety of a child or children, such as:

- Possible presence within the family environment of a Person Posing a Risk to Children;

- Presence of known risky behaviour, such as drug and alcohol abuse;
- Where there are reasonable grounds to believe that information given by a family as part of the assessment is misleading or untrue e.g., the claimed separation of a couple where domestic abuse is known to be a significant risk factor.

This approach has been advocated recently in court cases and a serious case review/ Child Safeguarding Practice Review (CSPR).

In the 2017 **Serious Case Review in relation to Child G**, the following learning was identified (para 1.3):

'When conducting assessments and reassessments of vulnerable families, practitioners may find that including internet and social media checks would enhance and triangulate information given by parents.'

The rationale stated to underpin this learning is that:

'Checks on the internet and social media can provide publicly available information about lifestyle and relationships to inform assessments.'

The review report also noted that:

'…Such checks, including on social media, in other cases could, for example, contradict denials of contact with dangerous ex-partners.'

The Review included a Recommendation that the Safeguarding Boards involved:

'Consider how best to enable practitioners to access and use relevant internet and public facing social media content to enhance their assessments. This should include policy and practice guidance.'

A more recent analysis of findings from CSPRs can be found in The Child Safeguarding Practice Review Panel Annual Report 2022-23 (publishing.service.gov.uk)

The **Cafcass Social Media Policy** counsels that 'practitioners should be aware of the complexities around authenticating online information. Screenshots and printouts can be manipulated by editing the information, and practitioners should also question the trail of how and where the information was found.'

2.2 Service of Court Documents

The Honourable Mr Justice Holman, in the case of **Re: T (A Child) [2017] EWFC 19** said he wanted the judgment to highlight that social media may be a useful tool for tracing parents who are being served with notice of adoption.

'So, I do wish to highlight by this short judgment that, in the modern era, Facebook may well be a route to somebody such as a birth parent whose whereabouts are unknown and who requires to be served with notice of adoption proceedings. I do not for one moment suggest that Facebook should be the first method used, but it does seem to be a useful tool in the armoury which can certainly be resorted to long before a conclusion is reached that it is impossible to locate the whereabouts of a birth parent. Of course, not everyone is on Facebook but, in this particular case, a relatively socially disadvantaged young mother …. has been found very rapidly by that means. (paragraph 21)'

The **Cafcass Social Media Policy** available at Social media guidelines | Cafcass states that 'We will never share information or engage in discussion about individual cases in the family court on social media. Please do not post case information on social media.' Further, Cafcass states that 'We may record information posted to social media accounts and use that information for reporting, record keeping and monitoring. No attempt will be made to further identify people, except where requested and authorized to do so by the law.

In rare circumstances, we may be directed by the court to contact an individual via a social media channel. This will be done as discreetly and sensitively as possible. Contact will always be made through our official accounts. Please do not respond to individual accounts claiming they are acting on behalf of us.'

These guidelines cover all Cafcass social media accounts:

- Twitter
- Linkedin
- YouTube
- Facebook

These also cover blog comments at www.cafcass.gov.uk

2.3 Searching for service users via social media

Issues

The increasing use of social media sites brings with it additional considerations. These include:

- Confidentiality and consent of service users;
- The need to process personal data in accordance with data protection principles;
- Professionals' own right to privacy and private life;
- The need for caution and corroboration – social media accounts can be infiltrated/faked. Service-users may have more than one online persona;
- Appropriate arrangements need to be made for setting up dedicated social media accounts. It is not appropriate to use professionals' personal accounts or 'fake' accounts. Employers may wish to set up corporate private profiles with access limited to a small number of staff.

2.4 Data Protection

Information gleaned from searches of social media sites will constitute 'personal data' which must be processed in accordance with data processing principles. It must be:

- Processed in a way that is lawful and fair;
- For specified, explicit and legitimate purposes;
- Adequate, relevant and not excessive;
- Accurate and kept up to date;
- Kept for no longer than is necessary;
- Processed in a secure manner.

2.5 Consent

It is good practice, where enquiries are likely to include searches of social media sites, to make service-users generally aware of this fact by including this in the information which is given to them at the commencement of the process, for example at the commencement of the Assessment.

In specific cases, social media searches, as with other forms of information-gathering for Assessment purposes, should generally take place with the consent of the subject, unless there are valid reasons to the contrary. There may be an 'overriding public interest' in obtaining and sharing information without explicit consent. This will depend on the circumstances of each case. For more information, see: **Confidentiality Policy**.

2.6 Covert/Overt Surveillance and the Regulation of Investigatory Powers Act 2000

Viewing a service-user's social media content without their specific consent is not necessarily, of itself, unlawful.

However, consideration must be given, in all cases, as to whether viewing the sites constitutes 'directed surveillance' under the Regulation of Investigatory Powers Act 2000 ('RIPA') and so requires authorisation under that Act. This is a complex area.

Whilst the following general principles apply, each case must be treated on its own facts, and legal advice MUST be sought as necessary:

- If the consent of the service-user is obtained, then no further authorisation would be required;
- If consent is not obtained but no privacy settings are in operation to prevent viewing, then the material available on the sites can be regarded as 'open source', and so a **single** viewing would not constitute 'directed surveillance' under RIPA and no authorisation would be required under that Act;
- However, the Chief Surveillance Commissioner (now superseded by the Investigatory Powers Commissioner) made clear his view that **repeat** viewing of sites by staff may constitute 'directed surveillance' and if done covertly (i.e., without the knowledge of that person) then this would be 'covert surveillance'. This would require authorisation under the Act in the form of a warrant from a magistrate. * It is for the employer to ensure that any covert surveillance is properly authorised, recorded and, most importantly, legally justifiable.

*(The Protection of Freedoms Act 2012 amended the regulation of investigatory powers legislation to reduce the circumstances in which a surveillance authorisation under RIPA can be granted by a local authority, rather than by a court. A local authority can now only grant an authorisation under RIPA for the use of directed surveillance for the investigation of criminal offences which attract a maximum custodial sentence of 6 months or more or relate to the underage sale of alcohol or tobacco. Surveillance as part of any other investigations, e.g., child welfare/protection, can only be authorised by a court).

What constitutes 'repeat viewing' is not set out and will depend on the facts of each case.

3. Communicating with service users via social media (i.e., WhatsApp)

Frontline professionals have indicated that service users have expressed a wish to be able to communicate via WhatsApp rather than text message or emails.

This will assist frontline professionals with delivering the best and most responsive service possible to service users.

WhatsApp is a third party application which cannot be secured within HCC systems. Therefore, there is a need to ensure clear boundaries around use and content to minimise the risk of sensitive data being shared inappropriately.

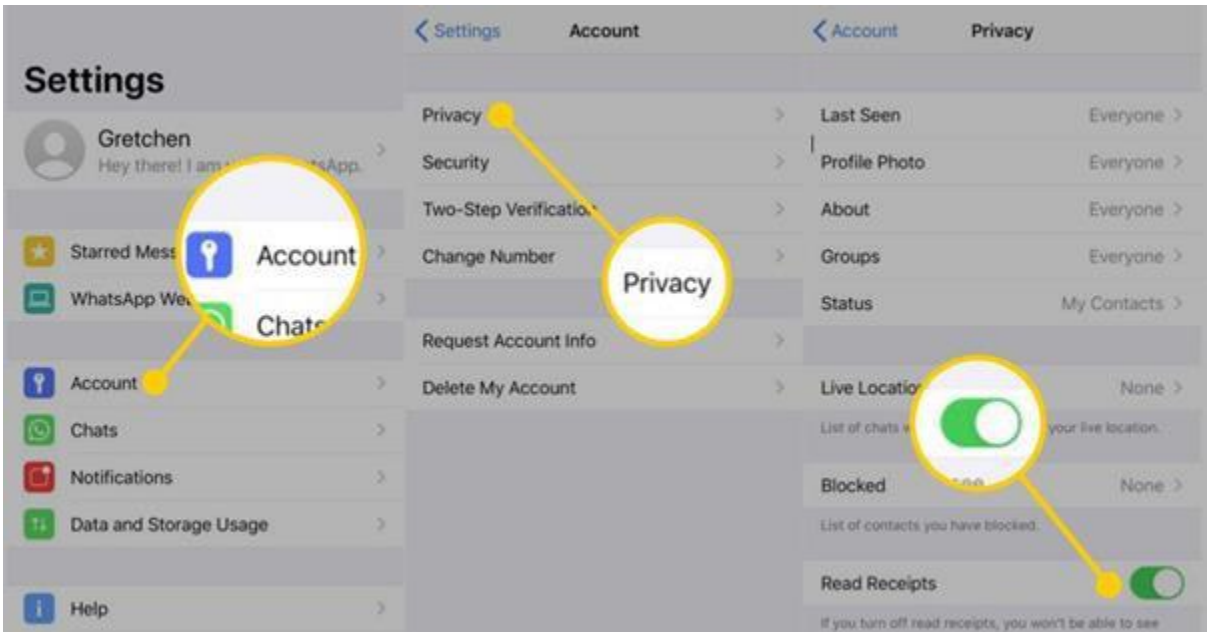
Staff must recognise that there are clear vulnerabilities in using this method of communication with service users and only use it where absolutely necessary. Ensuring you have the latest version WhatsApp will protect against newly discovered vulnerabilities.

3.1 HCC ICT Acceptable Use Policy

Staff are reminded that the use of WhatsApp and their mobile device should be in line with the ICT Acceptable Use Policy and staff are asked to pay particular attention to Section 2 regarding responsibilities.

3.2 Security settings

In order for clients to not be made aware when their allocated worker is online or has read their message, staff must ensure that the privacy setting within WhatsApp is changed to disable this function.



On:

- Android: Tap More options > Settings > Privacy;
- iPhone: Tap Settings > Privacy;
- KaiOS: Press Options > Settings > Account > Privacy;
- Desktop: Click Menu > Settings > Privacy.

You can change who can:

- See your Last Seen and Online;
- See your Profile Photo;
- See your About information;
- See your Status updates;
- See Read Receipts;

- Add you to Groups.

Note:

If you don't share your last seen or online, you won't be able to see other users' last seen or online.

If you turn off read receipts, you won't be able to see read receipts from other users. Read receipts are always sent for group chats.

If a contact has turned off read receipts, you won't be able to see if they've viewed your status updates.

People online in a chat thread with you can see when you're typing.

Private and professional accounts must be kept separate and not linked in any way. Staff must only communicate with service users using their HCC device and account.

3.3 Time boundaries

There is a need to be clear with expectations relating to times of communication and ensuring that staff only communicate with service users and foster carers during their normal working hours. The time boundaries must be communicated to service users to manage expectations.

Staff should usually only send WhatsApp messages between 8.30 am and 5.30 pm Monday to Friday, or normal working hours if part time (WhatsApp does not have the functionality to restrict working hours). It is recognised that some communications will take place during the early evening. Staff should not be using WhatsApp to communicate over the weekend, although there may be some exceptions to this within residential care which should be agreed with your line manager.

Service users will also be asked to only message during normal working hours, however, it is acknowledged that they may not always comply with this request. There is no expectation that the message will be responded to until the next working day.

Staff are encouraged to turn their handsets off at the end of their working day (unless on duty).

3.4 Content in written communications/messaging

WhatsApp must not be used for discussions that may include any sensitive content that is identifiable to the service user or anyone else.

WhatsApp is to be used for communications between staff and service users such as confirming appointments, meetings, receiving a request from a service user to call them and providing information that is publicly available already (e.g., signposting helpful websites).

Staff must remember that, although WhatsApp is an informal method of communication, all messages must remain professional and written and verbal communication must be conducted within appropriate professional boundaries.

Don't use WhatsApp for communicating or recording information that must be retained for statutory or records management purposes, such as authorisations or approvals.

Service users must be asked to communicate appropriately with no names mentioned in conversations and any sensitive information to be discussed either face to face or verbally on the phone. If this is not complied with, they must understand the option to communicate in this way may be withdrawn.

3.5 Video and audio calling

WhatsApp has the functionality to make both video and audio calls, and this can be used with service users.

Staff are asked to ensure that Wi-Fi is used wherever possible for these forms of communication to minimise the use of data. Staff must be aware of where they are making video calls and what information about themselves, they are sharing.

Staff are reminded of their responsibilities within the Driver Risk policy which states a mobile phone must not be used whilst driving for work.

3.6 Consent

All service users must provide written consent to confirm that they authorise this form of communication with their allocated worker, and they are aware of how we will use the information they provide using WhatsApp. A Privacy Notice has been completed and will need to be shared.

The consent form will need to be uploaded to the relevant case record on LCS.

In order to enable the use of WhatsApp, staff are required to send the following message at the point where communication in this form commences with anyone:

The content of the messaging conversations will be processed as part of our statutory responsibility for the well-being and safety of children and support for families. This is what

is known as our “Public Task”. If you do not wish to use WhatsApp for this purpose or you change your mind, we will not contact you this way again.

Please confirm if you are in agreement to use WhatsApp for this purpose.

Further Information

Social Work England Professional Standards

Serious Case Review: Child G

Cafcass Social Media

Guidelines

Re: T (A Child) [2017] EWFC 19

Covert Surveillance and Property Interference Code of Practice

Hertfordshire County Council Social Media Policy

Hertfordshire County Council ICT Acceptable Use Policy

Podcast: should social workers be on social media? - Community Care

Social workers using social media to find evidence on service users as lack of guidance leaves knowledge gaps (communitycare.co.uk)

social-work-and-child-protection-beyond-the-covid-19-pandemic_web.pdf (researchinpractice.org.uk)

Using social media in social work assessments: what the evidence tells us (communitycare.co.uk)

The dos and don’ts on social media for social workers (communitycare.co.uk)

Why and how social workers should use social media (communitycare.co.uk)

Avoiding the pitfalls of WhatsApp (localgovernmentlawyer.co.uk)

Additional Information

whatsapp-in-government.pdf (instituteforgovernment.org.uk)

Behind the Screens (ico.org.uk)

Social media guidance for councillors | Local Government Association