On-line safety

Guidance for staff in Children and Families

Version: 2.0
Date Issued: June 2020
Review: May 2022
Team: Practice Improvement Team
Protective Marking: Internal

Contents

1. About this document

1.1 Social media is used more and more to communicate with others both personally and in the working environment. It helps people to connect with each other with shared interests, keep in touch with friends and colleagues. It is a great way to bring together groups of people working on the same project, for example, and to share views and opinions.

1.2 Using technology to facilitate 'everyday communication' is now the 'norm' for many professionals, parents and young people. However, within this scenario the practitioner will have a dual 'persona' if you will. An electronic self that is 'personal' and an electronic self that is 'at work'.

1.3 While there are many benefits in using social media, it is important that practitioners use it within the standards set for social workers in Warwickshire. This guidance helps to identify potential risks in the use of social media.

1.4 Any breaches of this guidance could result in an employee being referred to the disciplinary procedure.

1.5 This document is aimed at all social care practitioners and managers, as well as social workers and qualifying social work students and should be read in conjunction with the following documents:

- Information Compliance Policy
- WCC personal data confidentiality agreement (DOCX, 51 KB)
- Council's Information Compliance Policy and associated standards and procedures for the handling and security of information.

1.6 This guidance does not cover technical details for configuring or using specific software apps. Any questions relating to technical aspects or use of apps, should be addressed to WCC ICT department.

2. Aims

2.1 This guidance aims to:

- Ensure safeguarding children in the digital world is a priority;
- Maximise the participation of children, young people and families with the services that Children and Families provide in a way that they find most accessible;
- Assist employees to work safely and responsibly within a framework of best practice;

- Set down the standards of behaviour that the Children and Family Service expects from its employees;
- Minimise the risk of allegations being made against employees about inappropriate behaviour;
- Project a clear message that unlawful or unsafe behaviour is not acceptable;
- Establishes a culture that safeguards children, young people and C&F employees

3. Social media and its professional implication

3.1 For the purpose of this guidance, social media means the online platforms used to engage, to create relationships, have conversations and communicate with others. It's the content that users upload to platforms like Facebook, Twitter, Instagram, YouTube, WhatsApp, Snapchat etc. It could be posting a comment, video or photograph or replying to other people's posts or a blog, video, podcast, for example.

3.2. When using social media and digital technologies, practitioners should consider and apply professional standards; examples include:

- to actively listen to understand people, using a range of appropriate communication methods to build relationships.
- to establish and maintain skills in information and communication technology and adapt their practice to new ways of working, as appropriate;
- not to use technology, social media or other forms of electronic communication unlawfully, unethically, or in a way that brings the profession into disrepute.

3.3 Section 3 of WCC Employer and Employee Responsibilities Code (DOCX, 37 KB) expects employees to follow the same standards with their online presence as they would in any aspect of their lives and should:

- Be aware that postings on social media sites can be accessible to a very wide audience and can remain available for a very long period of time.

- Take great care not to post anything that may be considered as bringing the council into disrepute or posting anything that another person may find it to be offensive, disrespectful or discriminatory nature towards the council, managers, staff, clients or associated people such as partner organisations or contractors.

- Be aware that it will not be an acceptable excuse to claim that such postings are private i.e. even if it can be shown that they have been made from a personal device and in the practitioner's own time.

- Be aware that the council monitors the use of its own equipment. WCC devices must not be used to post to personal social media accounts.

3.4 Be aware when using social media of the statement in 2.3.3 of WCC Employer and Employee Responsibilities Code (DOCX, 37 KB) – all officers of the Council are required to be politically neutral while at work and it is important that you show no bias or personal preference, whatever your personal beliefs may be.

3.5 Practitioners MUST not disclose or post any personal information about customers or employees i.e. details of their customer/employee record. This will be considered as a data breach in line with WCC Confidentiality agreements - Confidentiality clause for staff - clause 20 terms of employment states:
"You may have access to and handle confidential information relating to individuals, staff, other parties and Council business, during your employment. The information must be kept accurate, factually correct and handled correctly and securely. You must not whilst you are employed or after your employment ends disclose to any unauthorised person, that confidential information except where permitted by law, or authorised by the Council."

4. Video conferencing and WhatsApp

4.1 Due to the increasing concerns regarding the spread of the Covid-19 pandemic, Children and Families are promoting the use of Microsoft Teams and WhatsApp to enable the use of video conferencing as a medium for completing 'visits' with parents and direct work sessions with children and young people. The individual needs of each child is risk assessed to enable managers to decide whether our contact with them and their family/carers may be completed by "virtual visits" or actual visits. If it is agreed that virtual visits are appropriate, then practitioners should routinely ask families to identify their preferred available video conferencing application (Microsoft Teams and WhatsApp) in order to reduce the need for face to face contact.

4.2 Parents, children and young people will have different confidence levels with regards to technology. They may view the different apps as a tool used with friends and family and not necessarily their social worker. While children generally are familiar with video conversations and usually are comfortable

with technology, they may feel under pressure to behave in a certain way during a video call, they may become over excited, angry or upset, worried or scared or may feel reluctant to engage.

4.3 The use of video calls for communicating with young people, workers, parents and carers. This needs to be assessed to ensure that is right for the individuals involved. Once this has occurred, it can enable improved opportunities for supporting family time, frequent contact between parents and the carers/workers. This can support, when working well, the progressions of plans for children. However, the worker must also review the activity and any risks to ensure that this communication is still supporting the child and young person's wellbeing. There is no one-size-fits-all approach.

Best practice information, guidance and support for practitioners and managers about ethical, practical, and professional aspects of video call/contact and virtual/online home visits has recently been developed by The PCFSW & Social Work England - Best Practice Guide for Video Call/Contact and Virtual/Online Home Visit

4.4 Practitioners can also refer to WCC corporate guidance in relation to virtual meetings together with Etiquette for Successful Virtual Meetings which provides some guidance on how to get the best from a virtual meeting.

5. Using email, mobile phones, instant messaging and social networking sites

5.1 The following points must be adhered to when communicating using information communication technology:

- Only use devices contracted to/provided by Warwickshire Council e.g. mobile phones, office phones, pc's / tablets.
- Only use email addresses, instant messaging identities or social networking accounts that have been formally established and approved by Warwickshire County Council for professional purposes.
- Friendly banter between an employee and a young person is not necessarily inappropriate, but it can look very different if carried out using email, text messaging or instant messaging and might lead to difficulties if misinterpreted, forwarded or used out of context. Employees must be careful not to take risks in their communications with children and young people to avoid any possible misinterpretation of their motives or any behaviour which could be interpreted as grooming.

- Personal e-mail addresses, instant messaging identities, social networking accounts or home/mobile telephone accounts must not be used to contact children or young people without the explicit agreement of the employee's line manager. All details must be recorded in Mosaic and 'signed off' by a manager with a logged activity decision.
- Employees should be aware of and comply with the Warwickshire County Council's policy on the use of email, internet and social media.
- In all instances where email, text or instant messaging is used by an employee to communicate with a child or young person, it must be recorded electronically on Mosaic as an activity. It must be explicit that this is a virtual visit and the content of the 'visit' should be recorded as any other type of visit.
- Take care when establishing usernames and automatic signatures to ensure that they are appropriate for communicating in a professional setting.
- Some instant messaging applications have a facility to record a log of conversations which could be used to protect an employee in case an allegation is made. These should be uploaded into the person's Electronic Social Care Record (ESCR)

6. Do's and Don'ts when using social media

6.1. Points to consider when posting information online

- Do think about whether it is something you should be sharing.
- Do not share it online if the information is confidential and is about a person who uses Children and Families s services, their family or carers.
- Do not post any information or views that reflect negatively on you, your employer or the Children and Families service profession.
- Do minimise the amount of client identifiable data communicated via instant messaging;
- Do think carefully about the information you work with when using WhatsApp - what would happen if the mobile device was lost, or it's stolen? Suppose the voice/video calls were overheard in a cafe or read from the screen on a crowded train. Could there be damaging consequences? If the answer is 'No', then it's probably OK to use WhatsApp to communicate that information with colleagues.

6.2. Maintaining boundaries

6.2.1 Using social media can create risks, particularly where personal and professional boundaries become unclear:

- Think carefully before accepting friend requests from people who use our services. If you know someone because they use our services, you shouldn't become friends with them;
- If a person who uses our service, their family or carer contacts you about their care or other professional matters through your private profile tell them that you cannot mix social and professional relationships, and offer an appropriate alternative communication channel
- Do not use social media to discuss people who use social services or their care with them or anyone else.
- Don't use the instant messaging conversation as the formal case record: all case records should be recorded in line with policy on Mosaic and ensure original messaging notes are deleted.
- Do not allocate work or tasks to colleagues or business support staff via WhatsApp groups or text messages.
- Don't allow anyone else to use your device at any time.

6.2 Protect yourself

6.2.1 Other people can easily find and see your personal information and profiles as well as the posts on your social media:

- Think about how accessible you are online. For example, you can limit who can read your posts and turn off the ability for your profile to appear in online searches.
- You can also make some accounts private like Instagram and Twitter.
- However, social media sites do not guarantee confidentiality whatever privacy settings are in place.
- Remember to update your privacy settings regularly.
- Do set mobile devices to require a passcode if it is being used for this purpose;
- Do switch on additional security settings such as two-step verification;
- Do set message notifications to private and disable banners on the device's lock-screen;
- Do ensure you are communicating with the correct person or group, especially if you have many similar names stored in your personal device's address book
- Do take care when selecting the membership of the group if you are an instant messaging group administrator, and review the membership periodically
- Do separate groups that share client or operational information from social groups
- Do review links to other apps that may be included with the Instant Messaging software and consider whether they are best switched off

- Do remember that losing your phone now has professional ramifications as well as personal
- Do remember that instant messaging conversations may be subject to Subject Access Requests and potentially Freedom of Information requests
- But above all, remember that everything you post online is public. People can easily find, copy and share your posts without you knowing. Everything you post online can be traced back to you and there is a permanent record, even after deleting it.

6.3 Threatening or abusive posts about a member of staff

6.3.1 If any member of staff believes they have been subject to harassment or a specific threat on a social media platform they should inform:

- Their line manager
- Their local HR business partner

6.3.2 Further information is contained within Bullying and Harassment Procedure on the management of unacceptable behaviour. This includes guidance on determining what is opinion or criticism, and what is harassment or threatening behaviour; and the steps for managers to follow when an incident is reported.

7 Behaviour when using social media

7.1 Professionalism

7.1.1 Practitioners have a duty of confidentiality and a responsibility to safeguard any council information or data that they access, and it should be treated as OFFICIAL information. Practitioners are trusted to make a reasoned judgement about whether it's safe to use WhatsApp or whether they should use a different work tool provided by Warwickshire County Council

7.1.2 Text messages are considered professional communications and should be noted on the client’s case record, as well as any responses received and the time and date.

7.1.2 Practitioner’s should use similar terms to those they would use in emails or letters. Avoid abbreviations or 'text speak'.

7.2 Inappropriate behaviour

7.2.1 Think about this in respect of professionalism and being a role model. The scope here is enormous bearing in mind that actions outside of the workplace could be considered a fundamental breach of trust and confidence placed in the employee and may constitute gross misconduct. Examples include:

- Posting offensive or insulting comments about Warwickshire County Council or the Children &Families Service;
- Making derogatory comments about children, young people and their families or any work colleagues on social networking sites;
- Trading in sexual aids, fetish equipment or adult pornography;
- Accessing adult pornography on work computers;
- Making political statements.

7.3 Inappropriate material

7.3.1 Inappropriate is a term that can mean different things to different people. It is important to differentiate between ‘inappropriate and illegal' and 'inappropriate but legal'. All employees need to be aware that in the former case investigation may lead to criminal investigation, prosecution, dismissal and barring. In the latter it can still lead to disciplinary action, dismissal and barring even if there is no criminal prosecution.

7.4 Illegal material

7.4.1 Accessing (viewing) making, storing (possessing) or disseminating indecent images of children on or off the internet, whether on or off work premises is illegal. If proven this will lead to criminal proceedings and the individual will be barred from working with children and young people. Sharing adult pornography with children is also illegal.

7.4.2 Possessing or distributing indecent images of a person under 18 can include viewing such images online. This may also constitute possession even if they are not saved.

8 Storage and data retention

8.1 Laws and regulations make Children and Families and its employees responsible for managing information. Some examples include:

- the Freedom of Information Act
- the Data Protection Act and General Data Protection Regulation
- the Public Records Acts

8.2 When C&F’s receive a request for information, they need to know where all the relevant information is held. Storing business information on appropriate council approved systems helps because WCC can provide evidence about decisions made and understands the information held, and where to find it;

8.3 Always store WCC information in WCC systems. If practitioner's use WhatsApp or other social media platforms to discuss work topics, make sure the key information is also stored in an appropriate case recording. Always remove any redundant information from WhatsApp by clearing/deleting conversations.

8.4 WhatsApp allows data to be exported. It can then be store on an appropriate WCC system. Make sure that only the correct people have access to the information. This is important after staff or organisational changes, for example.

8.5 For more guidance, see WCC Information Framework.

9. Further information

9.1 Please see the following guidance to support utilising Microsoft Teams and WhatsApp technology.

- Microsoft Teams - Quick Start Guide
- Joining a MS Teams Call - External User
- Scheduling a Teams Call - External Guest User
- How to create a Teams meeting
- How to download Whats App to your WCC mobile device