## Guidance on the use of mobile communication and social media in Children's Services

**Introduction**

1. Gloucestershire County Council (the Council) accepts that communicating to service users via mobile devices is essential to enabling the Council to meet its aims and objectives. It is a requirement that your use of the Council's corporate devices is legal and appropriate for delivering Council services and does not create unnecessary business risk.
2. The Council’s mobile devices are made available to users for Council business purposes. Limited personal use is permitted provided that such use is strictly in accordance with council policy.
3. Where Social Media is required to be used to communicate with children and families, it must be done in line with the Council’s various Information Security policies.
4. The council recognises that social media now helps to shape the culture and identity of young people, this forms a part of the assessment process and how we support and educate the children and families in their use and understanding of social media and the risks associated.
5. Social Work is practice led but must abide by Information Security policies. Staff should also understand and pay particular attention to this guidance as the reasons for requiring a policies and guidance is to keep service users and staff safe.

**Risk Management**

The Council recognises that there are risks associated with the use of mobile communication, and the extensive damage that can be caused by misuse. This guidance aims to ensure appropriate access to, and use of, the Council's corporate devices to help mitigate the following risks:

* Harm to individuals
* Damage to the Council's reputation
* Potential legal action and/or fines against the Council or individual(s)
* Inappropriate use of council resources
* Viruses and other malicious software
* Service disruption

**Scope**

1. This guidance applies to workers in Children's Services who communicate to service users via a corporate device, including but not limited to WhatsApp and text messaging.
2. All users are expected to comply with this guidance at all times.

**Use of GCC equipment**

1. You must ensure that you have the appropriate encryption on your GCC devices, with an unlock pin enabled.
2. Do not store messages/voicemails/ photographs / videos on the device, these must be recorded on the relevant system (LiquidLogic/Capita) or stored securely within 24 hours and then deleted from the device.
3. If you need to save contact details, keep these minimal with the name and number only.
4. It is your responsibility to keep the device safe and secure, if the device is lost or stolen, report to the [Information Management Security Team](mailto:informationsecurity@gloucestershire.gov.uk).
5. Staff to be aware of the [ICT equipment use policy](https://www.gloucestershire.gov.uk/media/2086280/ict-equipment-policy-v11.pdf).
6. You must return the device to your manager when you end your employment.

**Communicating with service users**

The Council recognises the benefits of being able to communicate with service users through methods of text messaging but there are risks that need to be managed when doing so.

Ensure you have discussed and agree with the service user the method of communication. You must ensure they are aware that when using these platforms for communication the data is out of our control and in terms of security this is in the hands of the relevant platform.

**Remember – do not store data on the device. Ensure data is recorded on the relevant record (i.e LiquidLogic/Capita).**

All guidance and policies should be followed in conjunction with the latest visiting guidance for the service area.

1. **Text messaging / instant messaging**

* Groups including service users must not be created, and you must leave if you are added to one. Exceptions to this are where the worker has created a group for the delivery of controlled, short life work for a specific purpose with appropriate consent from those involved.
* Photographs and videos must not be transferred between worker and service user. Service users can send photographs and videos but you must not send any in return.
* Personal mobile devices must not be used to communicate with service users or colleagues containing personal and/or sensitive information.

1. **Video call**

* This can be a positive method for face to face communication, but considerations need to be made of who could overhear the conversation.

1. **Audio call**

* Be aware of who else may hear the phone call around you or the other person. Do not have the call on loudspeaker if you are in public.

**Social Media**

1. **Use of own personal social media**

* Do not befriend service users from personal social media accounts.
* Have appropriate security settings in place so you account is not visible to all.
* Ensure know how to take action if any online abuse is received (see part e)

1. **Looking at service user’s social media**

Gloucestershire County Council has taken the position that all covert surveillance will be regulated as if it met the threshold for the Regulation of Investigatory Powers Act (RIPA). This includes covert surveillance conducted by monitoring social media profiles. The RIPA framework helps the Council ensure it does not breach a person’s human rights when exercising its functions. The link below to the Council’s procedural guide for RIPA outlines the process for approval when it is deemed that covert surveillance is required as well as the consequences of carrying out unlawful surveillance.

[The Regulation of Investigatory Powers Act (RIPA) 2000](https://staffnet.gloucestershire.gov.uk/media/222130/ripa-procedural-guide-version-1.docx)

Undertaking covert surveillance should only be employed where there is no less intrusive method of gathering the evidence and is both necessary and proportionate to the seriousness of the matter under investigation. To avoid the potential for inadvertent or inappropriate use of social network sites in this way, Council officers should be mindful of the following:

* *Do not create a false identity in order to ‘befriend’ individuals on social networks without authorisation;*

*• When viewing an individual’s public profile on a social network, do so only to the minimum degree necessary and proportionate in order to obtain evidence to support or refute an investigation;*

*• Repeated viewing of open profiles on social networks to gather evidence or to monitor an individual’s status must only take place with RIPA authorisation;*

* *Be aware that it may not be possible to verify the accuracy of information on social networks and if such information is to be used as evidence, take reasonable steps to ensure its validity.*

1. **Using social media to communicate with service users**

* [Social Work England. Standard 5.6](https://www.socialworkengland.org.uk/media/1640/1227_socialworkengland_standards_prof_standards_final-aw.pdf) states “a*s a social worker I will not use technology, social media or other forms of electronic communication unlawfully, unethically, or in a way that brings the profession into disrepute.”*
  + This SWE standard should be viewed as applicable to all staff communications with service users and not just for social workers.
* Social media can be a supportive tool to facilitate communication in an online community. However, social networking sites such as 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.
* Staff 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.

1. **How to positively engage with young people around social media**

The Council is aware that young people use many different social media platforms, we need to be able to understand what these are and how to have conversations on how to best use them and the risks involved. The link below provides the up to date guidance on social media platforms and the age limits on these, how to discuss internet safety and the latest on different platform and how to keep children safe. Use the tools available to engage children and young people in conversations about social media, recognising it will form part of their identity.

<https://www.internetmatters.org/>

1. **Policies**

The two policies below include how to best use your own social media and what to do if you experience any bullying on social media.

[Social media use policy](https://www.gloucestershire.gov.uk/media/6773/social-media-policy.pdf)

[Cyber bullying on social media](https://staffnet.gloucestershire.gov.uk/media/221060/she-guidance-g088-cyberbullying-on-social-media-nov-18.doc)

**Responsibilities of Staff**

1. **User Responsibility**
2. Communication with service users must be consistent with the Council's Code of Conduct for Employees. All users are responsible for using the Council's corporate device appropriately and in accordance with the applicable policies and this guidance.
3. Records of actions or decisions made must be uploaded onto the relevant system (e.g. Liquid Logic) within 24 hours, and then deleted from the corporate device.
4. It is your responsibility to:
   * + - Ensure you read and understand this guidance as part of your induction to the Council.
       - Use the Council's corporate device in accordance with this guidance.
       - Use the Council's corporate device responsibly and in a way that will not harm the Council's reputation.
       - Recognise that the Council's corporate devices are provided for business use and must be protected from unreasonable and excessive personal use.
       - Report any misuse of the Council's corporate device. Details of how to do this are provided at Reporting / investigating a security breach.
       - Promptly report any loss or theft of any Council asset to the ICT Service Desk & Information Management Security Team, ensuring a police reference number is provided.
       - Report any abuse - The two policies below include how to best use your own social media and what to do if you experience any bullying on social media.

.[Social media use policy](https://www.gloucestershire.gov.uk/media/6773/social-media-policy.pdf)

[Cyber bullying on social media](https://staffnet.gloucestershire.gov.uk/media/221060/she-guidance-g088-cyberbullying-on-social-media-nov-18.doc)

1. **Manager Responsibility**
   * 1. Ensure the worker is provided with appropriate GCC encrypted equipment
     2. Carry out a minimum of two dip tests per year
     3. Ensure this is a live discussion through discussion as part of staff induction, team meetings and supervisions.

**Related Policies**

All available at [Information Management and Security Policies](https://www.gloucestershire.gov.uk/council-and-democracy/strategies-plans-policies/information-management-and-security-policies/)

* [Social Media Policy](https://www.gloucestershire.gov.uk/media/6773/social-media-policy.pdf)
* Code of Conduct for Employees
* Information Protection and Handling Standards Policy
* Internet Acceptable Use Policy
* Information/IT Access Policy
* Data Protection Policy
* Software Management Policy
* [Password Policy](https://www.gloucestershire.gov.uk/media/1519558/gcc-password-policy.pdf)

**Review and Revision**

This guidance will be reviewed as it is deemed appropriate, but no less frequently than every 3 years.

# Document Control

|  |  |
| --- | --- |
| **Owner:** | Tom Underwood |
| **Author:** | Gareth Heward & Tom Underwood |
| **Last Reviewer:** | Ben Crow, Information Governance Advisor |
| **Create Date:** | Dec 2020 |
| **Next review date:** | Nov 2021 |
| **Approval:** | Children’s SLT |
| **Version:** | 1-2 |

|  |  |
| --- | --- |
|  |  |