Guidance on the use of Social Media and Social Networking Sites for Children's Services

Background

This guidance applies to any work undertaken by Children's Services using social media to establish facts in a matter. Whilst social media and social networking sites can be useful sources of information, caution must always be exercised to ensure that any interference with the human rights of those being observed; specifically, the right to respect for private and family life under Article 8 of the Human Rights Act 1998 are necessary and proportionate.

The Regulation of Investigatory Powers Act 2000 (RIPA) provides a statutory framework for the authorisation and conduct of certain types of covert surveillance (unknown to the subject) operations to provide a balance between preserving people's right to privacy and enabling authorities to gather evidence for effective enforcement action.

Whilst such authorisations are available under RIPA, the protection they afford can only be used where the surveillance undertaken relates to the prevention or detection of criminal offences that are either punishable by a maximum term of at least 6 months' imprisonment or, relate to the underage sale of alcohol and tobacco.

Therefore, an authorisation under RIPA would not be available to social workers as any surveillance will be undertaken for child protection purposes. However, using a "RIPA Like" process will help support social workers, if challenged, over their use of social media as part of their investigations to evidence necessity and proportionality (the balancing exercise).

The "RIPA Like" process for Children's Services

Due to authorisations under RIPA only being applicable where there is an investigation of particular criminal offences, a RIPA Like process will need to be followed in order to justify any covert surveillance of social media. Prior to any surveillance being undertaken, social workers will need to obtain authorisation from their Team Manager.

In the following circumstances, social workers would need to be careful to follow the "RIPA Like" process and ensure that proportionality and necessity have been considered when:

- accessing an individual's social media profile(s) more than once to obtain information;
- undertaking on-going surveillance, for example, undertaking regular planned checks of an individual's social media profile(s);
- setting up a fake profile to monitor someone's social media profile;
- sending a "friend" or "follow" request to the individual to gain access to their private profile;
- using a pseudonym to join a private group;
- engaging with others online without disclosing your identity;
- asking friends, family or colleagues to monitor or gain access to the individual's social media for the purposes of obtaining information on your behalf.

The above list is non-exhaustive. The social work team will not hold any social media accounts under a false name. You should not undertake any surveillance that is more than a one-off activity, or that is an activity that the individual has not given their consent to you carrying out, without obtaining authorisation under the "RIPA Like" process.

Repeat viewing of an individual's social media may constitute untoward interference with a person's privacy. Whilst the carrying out of repeated viewing isn't illegal, there is a risk of such viewing being challenged as a breach of the individual(s)' human right to privacy and family life free from interference, therefore the "RIPA Like" process should be followed to allow you to evidence proportionality and necessity.

This could also discredit any information obtained by the repeat viewing, which may result in the information being deemed as inadmissible as evidence within public law proceedings.

Communications with children through social media

Where we are the child's corporate parent, our corporate parenting duties enable us to act as a parent, including checking a child's social media account. Where social workers use social media in a parental stance, they will need to obtain the child's permission by expressly stating to the child that they might check their social media account for purposes such as to see where they were last night and asking if the child agrees to this. This will amount to a direct agreement between the child and the social worker, and a record should be made of the discussion with the child confirming their permission has been given. In exceptional circumstances, like any parent, there may be situations where you will need to access the child's social media without their consent. If this is being considered, the "RIPA Like" process should be followed.

When interacting through social media, the child may decide to unfriend you or block you if they no longer consent to you accessing their profile. It is important that this is respected, and for social workers to employ boundaries in ensuring that they do not use social media outside of normal working hours. The child will need to be informed that social workers will not be available to pick up messages sent via social media outside of working hours and should be signposted to alternative points of contact for emergency situations.

Considerations for Team Managers when authorising conduct under the "RIPA Like" process

Where actions are taken that are covert, the individual will be unaware of the Council's proposed actions and so is unable to give their consent to the activity. This is why it is important to consider the above factors.

Care should still be taken where the actions are overt as this could at times still result in breaching an individual's human rights and therefore consideration of necessity and proportionality should always be exercised.

1. Is authorisation required for the activity?

First, consider whether the activity is, or has the potential to be intrusive or interfere in some way with the individual's private or family life.

If the activity is covert, authorisation will be required as the individual has no means to consent to the activity that is being carried out.

2. Is the activity necessary, and if so, why?

As above, even if the activity is overt (where the individual is aware of the activity), and this has been consented to, there is still the potential that their human rights could be interfered with.

There needs to be a legitimate purpose for carrying out the activity, for example for the purpose of safeguarding. Consideration must first be given to whether there are any less intrusive means of obtaining the information. If there is a less intrusive method, then that should be used.

Authorisation should not be given if the information sought can be obtained by other means that would not impose upon the individual's human rights.

3. Is it proportionate?

The Team Manager must be satisfied there are no other reasonable means of obtaining the information.

If the activity is necessary, for example, serving a purpose in safeguarding and risk, it must also be considered proportionate.

This requires consideration by the Team Manager as to whether the activity is proportionate to:

- The issue under investigation;
- The degree of anticipated intrusion on the individual and others (collateral intrusion); and
- Whether it is the only option available, other overt means having been considered and discounted.

Consideration should also be given as to whether the surveillance is an essential part of the investigation, and what type/quality of information obtained by surveillance of social media it is likely to provide.

The activity will not be proportionate if it is excessive in the particular circumstances or if the information sought could reasonably be obtained by less intrusive means.

In deciding whether to carry out an activity that may impinge upon the human rights of the individual whose data you are investigating, it is important to look at the **5W's**:

- **Why** is the surveillance necessary?
- **Whom** is the surveillance directed against?
- **Where** and **When** will it take place?
- **What** surveillance activity/equipment is to be sanctioned?
- **How** is it to be achieved?

4. What is the collateral intrusion?

What is the impact of the activity on others' lives and how will this be managed? For example, when looking at an individual's social media account, images and messages of third parties are not to be captured and will be disregarded where they are.

Records Management

A detailed record of all authorisations should be kept by the Team Manager.

There must be arrangements in place for the handling, storage and destruction of material obtained through the use of any covert surveillance. Confidential material must be destroyed as soon as it is no longer necessary. It must not be retained or copied unless it is necessary for a specified purpose.

Further reading:

- Article 8: Private and Family life of the European Convention on Human Rights
- Office of Surveillance Commissioners 2016 Guidance

Appendix 1: Form to be used by social workers when undertaking "RIPA Like" work:

Wiltshire Council

REQUEST FORM FOR ONGOING OR REGULAR ACCESS TO SOCIAL MEDIA ACCOUNTS IN CONNECTION WITH CHILDREN'S SERVICES WORK

Full Name of requestor:

Role:

Team Manager:

Case number:

Name of child[ren]:

Who is the subject of the viewing?

(Please detail who the individual is)

What are you intending to access, and how often?

(Please give details as to the type of activity for which you are seeking authorisation – for example, Facebook account viewing once per week)

Why is the viewing considered necessary?

(Please give a brief description as to why the viewing of the individual's social media is necessary - for example, for safeguarding purposes)

Is there likely to be any collateral intrusion?

(Please detail any potential third-party information that may be viewed when carrying out the viewing of the individual's social media accounts) and how any 3rd party information is proposed to be dealt with)

Have you considered any alternative (less intrusive) options for obtaining the information sought?

(Please detail the options considered and why these have been discounted)

SIGNATURE:

DATE:

FOR COMPLETION BY TEAM MANAGER

NAME:

SIGNATURE:

DATE:

AUTHORISATION GRANTED: YES/NO

REASONS: