

Title/Status-	Policy
New document or revised	New
Date approved SMT	September 2019
Responsible Head of Service	Head of Safeguarding and Improvement
Date review	September 2020

Use of social media in social work investigations

Relevant legislation

- Human Rights Act 1998(HRA)
- the Human Rights Act 1998 (HRA);the Data Protection Legislation (the Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR) as amended, replaced or superseded from time to time.

1. .Introduction

1.1 This Policy sets out how social workers may use social media when carrying out their child protection duties under the Children Act.

1.2 The aim is to ensure that information gathering, investigations or surveillance involving the use of social media is conducted lawfully and correctly in accordance with an individual’s human rights and with due consideration of relevant legislation as set out above.

1.3 Use of Social Media in investigations refers to any instances where a Social Worker accesses Social Media as described to formally or informally gather evidence whilst carrying out their statutory child protection duties under the Children Act 1989.

2. Definition of Social Media for the purposes of this policy

2.1 Social media will always be a web-based service that allows individuals and or business to construct a public or semi-public profile (also known as social network services) and will often have some or all of the following characteristics:-

- the ability to show a list of other users with whom they share a connection; often termed “friends” or “followers”,
- the ability to view and browse their list of connections and those made by others within the system, and /or
- hosting capabilities allowing users to post audio, photographs and/or video content that is viewable by others.

2.2 Some current examples of the most popular forms of Social Media and therefore the most likely to be of use when conducting investigations, include: Facebook, Twitter, Instagram, snapchat, LinkedIn and YouTube.

3. Privacy Settings

3.1 The fact that digital investigation is routine or easy to conduct does not mean that relevant

legislation should not be considered. Care must be taken to understand how the Social Media website in question operates.

3.2 Any social worker using Social Media for investigation must not be tempted to assume that one service provider is the same as another or that the services provided by a single provider are the same.

3.3 Whilst it is the responsibility of an individual to set privacy settings to protect unsolicited access to private information, and even though data may be deemed published and no longer under the control of the author, it is unwise to regard it as “open source” or publicly available; the author has a reasonable expectation of privacy if access controls are applied. In some cases data may be deemed private communication still in transmission (instant messages for example).

3.4 Social Workers should not attempt to circumvent privacy settings and view an individual’s **information more than once** unless authorisation has been sought under the procedure set out in appendix 1 of this policy.

3.5 By setting their profile to private, a user does not allow everyone to access and use their content. This does not, however, extend to instances where a third party takes it upon themselves to share information which originated on a private profile on their own Social Media profile

3.6 Where privacy settings are available but not applied the data may be considered “open source” or publicly available (ie there is a reduced expectation of privacy). However in some circumstances privacy implications still apply. This is because the intention when making such information available was not for it to be used for a covert purpose such as investigative activity. **This is regardless** of whether the Social Media user has sought to protect such information by restricting its access by activating privacy settings. Viewing of the information as part of carrying out the statutory function of the social worker would therefore require the authorisation as set out in Appendix 1.

3.7 Investigations relating to a child’s welfare by a social worker carrying out their statutory functions are non-criminal investigations so they do not fall within the formal ambit of the Regulation of Investigator Powers Act 2000 (RIPA) but do fall within European Charter Human Rights considerations in particular Article 8, the right to respect for private and family life.

4. Authorisation

4.1 Certain activities (set out below in 4.8) require approval through a formal authorisation process which considers whether the use of covert investigatory techniques are an interference with the rights protected by ECHR Article 8.

4.2 The exception to this will be where a parent who is assessed to have capacity to give permission has given their clear and informed agreement to their social media information being accessed and used by the social worker as part of their ongoing involvement.

4.3 Where a parent has given consent to social media information being used either on a single or on multiple occasions this should be clearly recorded on the child’s record.

4.4 Where use is routinely part of supporting the child's welfare this may be set out explicitly within the child's current plan – including Child Protection plans, LAC plan, Pre-proceedings agreements and Care plans to court.

4.5 When seeking to access information from the social media account held directly by a child or young person the authorisation process should always been applied.

4.6 The authorisation process will consider whether the interference in the account holder's rights is in accordance with the law and if necessary in a democratic society so as to protect health or morals. For this purpose, there must be specific reference to the need to protect the welfare of a child.

4.7 Any interference must be proportionate requiring a balancing of the seriousness of the proposed intrusion against the seriousness of the matter being investigated and balanced with the availability of other means to information as part of the investigations.

4.8 Any use of social media by social workers as part of carrying out their statutory duties to gather information must be proportionate and lawful. Specifically, the following actions MUST be subject to authorisation in line with Appendix 1 of this policy: -

- Sending "friend" or follow "requests",
- Setting up a profile in an attempt to gain access to an individual's private profile or asking family, friends, colleagues or any other third party to gain access.
- Repeated and/or regular viewing (more than a single time) of "open source" content.
- Making contact through social media via a Covert Human Intelligence Source (CHIS) where this is likely to capture confidential information not available by any other means.

5. Record Keeping

5.1 Where authorisation is sought and agreed to seek information from Social media in line with the procedure as set out in Appendix 1, any evidence gathered which takes the form of any readable or observable content, such as text, status updates or photographs, can be copied directly from the site, or captured via a screenshot and copied onto a relevant electronic recording system. If necessary audio or video content can be captured.

5.2 When capturing evidence from a public Social Media profile, steps should be taken to ensure that all relevant aspects of that evidence are recorded accurately . For example, the time, date and status update should be visible on the screenshots.

5.3 When capturing evidence from a Social Media profile, steps should be taken to minimise the risk of collecting third party personal or private details alongside that of the person under investigation / suspected offender's, either before capturing the evidence, or subsequently through redaction.

5.4 Where relevant records are obtained during the course of an investigation they should not be destroyed but kept for as long as they are needed. They should be retained in accordance with the requirements of Data Protection legislation, the Freedom of Information Act 2000, Criminal Procedures and Investigations Act 1996 (ie consider using the evidence obtained in a sensitive unused material schedule) and any other legal requirements.

5.6 When information gathered under this policy is used to as part of evidence to court within care proceedings the rationale for use of social media information in the investigation should be explicit, including the authorisation that is in place. Liaison with the relevant legal advisor must take place when the process is applied in Pre-proceedings and court proceedings.