Accessing open source information about children and adults for safeguarding purposes

Introduction

The guidance is intended to assist when LA (LA or the LA) employees or others consider it appropriate to view and retain open source information for child safeguarding purposes. Family Court judges have recently criticised local authorities for not having reviewed publicly available material which is relevant to safeguarding issues. On the other hand the Chief Surveillance Commissioner wrote to all Local Authorities in April 2017 warning them of the risks of accessing "open source" material if this drifts into "covert surveillance".[1] This Guidance is designed to assist local authorities in their safeguarding function with achieving the correct balance and remaining within the law. The guidance covers digitally available information

Who is this guidance for?

[to discuss with LSB]

What is open source information?

Any publicly available information, including information responsive to Google or other search engine searches, information publicly available on social media such as twitter, Instagram, Facebook etc.

What is not open source information?

Information which is only available because you are a 'friend' of the target, information subject to privacy controls on Facebook or other social media, private communications such as texts to someone else, WhatsApp messages, private emails, direct messages on twitter.

This guidance is not concerned with anything other than open source information. If information is not readily accessible, it is not open source and you will need to seek separate

[1] Office of Surveillance Commissioners (now known as Investigatory Powers Commissioner's Office), *Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to the Scottish Ministers for 2016-2017* (published 20 December 2017), pg 21, paragraph 15.4 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/669953/OSC_Annual_Report_2016_-_2017.pdf accessed 8 February 2019

guidance/refer to the police who have the appropriate powers to obtain access to information which is not publicly available.

Legal issues

This guidance outlines general privacy rights, specific issues arising in the context of looked after children and local authorities, the criminal law issues and then provides summary guidance**.**

1. Outline of privacy and data protection rights

1.1. Local authorities and other public authorities are required to act compatibly with the European Convention on Human Rights (ECHR). Article 8 of the ECHR provides that:

(1). Everyone has the right to respect for his private and family life, his home and his correspondence.

(2). There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. [2]

1.2. The right includes the right to develop and maintain relationships with other people without unjustified interference.

1.3. The Human Rights Act 1998 (HRA) obliges public authorities to act compatibly with the Convention and gives the right to bring a claim where a public authority acts in breach of the requirements of Article 8 in a way which cannot be justified by Article 8(2).

1.4. This right has influenced the development of a free standing privacy right, misuse of private information, which gives a right of action against anyone misusing private information, not just public authorities.

---

[2] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR), Article 8

1.5. The principles applicable to both rights can be summarised as follows: Does the individual have a reasonable expectation of privacy in the information, or is it an activity within the ambit of Article 8(1)? If so, is there a public interest in its use and does the behaviour of the public authority comply with Article 8(2)? Is the use of the information proportionate? Is there a countervailing right (for example, freedom of expression or the need to protect a child) which should be balanced against the privacy right and which right should prevail in all the circumstances?

1.6. Where a LA acts in a way which is incompatible with the Article 8 rights of the individual, it must be able to demonstrate that its action is in accordance with the law under Article 8(2). The ECHR has said that this means that the legal framework must be accessible and clear. If the LA is monitoring social media in a systematic way, it must comply with the Regulation of Investigatory Powers Act (RIPA) which governs directed surveillance by public bodies and states that authorisation is needed and that surveillance should not take place otherwise.

Reasonable expectation of privacy

1.7. It is important to understand that some open source information can be considered private – the key test is whether there is a reasonable expectation of privacy in the information.

1.8. Information about children is given a higher level of protection than information about adults. For example, there can be a reasonable expectation of privacy in photographs of children in public places or other information about children, even if it is open source in the sense that it can be obtained by the public.

1.9. A substantial amount of the social media activity of children, particularly younger children, is likely to be considered to be their private information, even if privacy settings are not enabled allowing the information to be obtained by simple searches. Social media activity relates to the core areas of identity and social life protected by Article 8. The nature of the information is important – if it relates to sexual life, gender, criminal activity, money or any other area which

individuals like to keep private, then it should be assumed to be private. It is also important to consider where the activity portrayed takes place. Photographs tend to be given additional protection because they can be so revealing.

1.10. It is safest to think of all information on childrens' social media as being potentially private. For instance *photos of a 13 year old dancing in their bedroom posted on Facebook by that person should be considered private, even if the privacy settings allow the photos to be accessed and viewed by anyone searching. A posting by a 17 year old announcing his new job to the world may not be private information.*

1.11. Public domain information about adults is less likely to attract privacy protection. *For instance, newspaper articles about a conviction, interviews given by that adult, some social media postings if it is clear that the adult has capacity and intends the posts to be made public.*

Accessing and using open source information

1.12. Information in the public domain which is not private can be used freely. Information in the public domain which is private, can still be viewed and retained, but only for safeguarding purposes or for another public interest purpose such as the disclosure of wrongdoing, and the use needs to be necessary and proportionate to the purpose.

1.13. However, any private information (including on publicly available social media accounts) which is viewed on repeat occasions without the target's knowledge is likely to be considered covert direct surveillance and will be unlawful unless there is specific authorisation for it in accordance with RIPA. This is considered in more detail below.

1.14. If there are safeguarding concerns about a child's behaviour, or that they are being groomed, it may be justifiable for those with safeguarding responsibilities

which extend to a responsibility to make investigations into a child's welfare to look at the child's publicly available Facebook profiles, tweets or Instagram posts, even if they contained information in which the child might have a reasonable expectation of privacy, as part of an assessment of needs or risk. It might also be justifiable for that person to look at an adult carer's publicly available social media information in order to inform that assessment. If something caused concern, it may be necessary to reveal information further to the appropriate person [**NB this guidance does not deal with who the appropriate person would be in any specific situation and advice should be obtained**]. However, that information should not be used for any other purposes as that would take it outside the ambit of a public interest defence.

Examples

1.15. *A social worker is concerned that a vulnerable 15 year old girl is being groomed by a gang and wants to search for any evidence of her associating with gang members. A search of her social media and google searches reveals that she has been dressing up and making dance videos with her friends at one of their houses. This information is likely to be private information because of the vulnerability of the girl, her age, the fact that it involves photographs of young people taken inside someone's home. There was a good public interest and safeguarding reason for conducting the search and reviewing the social media. Once it appears that there is no good reason to be concerned about the girl, the fact and results of the search together with the public interest justification should be noted. There should not be recurrent searches and the images should not be kept. The images of the other children in the video are their private information and there is no public interest in retaining those images or disclosing them or keeping a note of the identities of others in the video.*

1.16. *If a social worker is concerned that a mother may be harming her child, it may be necessary to search the mother's social media and other public domain information to see if there is any evidence of the mother's conduct as it relates to her child which might assist social workers to make safeguarding decisions. The search reveals that the mother has a previous unspent conviction for assault and her open social media history includes numerous photographs of her*

outside hospitals. That information is public domain and not private and may reveal wrongdoing and is in pursuit of a proper safeguarding objective. There is no issue with using this information, storing it or disclosing it in accordance with usual safeguarding practice and guidance.

1.17. If searches of open source information including social media become systematic, that is if there are repeat searches targeted at the same individual so as to amount to surveillance, this will require RIPA authorisation if the target is not aware.

Consent

1.18. In some circumstances where a child is in the LA's care it will be appropriate to agree restrictions on and monitoring of the child's own social media use, or agree to monitoring of social media content with the child and/or the person with parental responsibility, in order to keep the child safe. Where the child is in care, there is a statutory duty to consult with the child.[3] Similarly sometimes an LA may seek consent to monitor social media use in the course of a safeguarding assessment.

1.19. If appropriate consent to monitoring or reviewing of private information (including some open source information as above) is obtained from a child or adult, the issue of privacy does not arise. Where the child is in care there is a statutory duty to consult with the child and it would be good practice to also consult with a child when an investigation is being undertaken. The consent has to be informed and freely given and the person consenting must have capacity to consent and understand exactly what they are agreeing to. It may sometimes be necessary to obtain both the parent and child's consent (see further below). The subsequent monitoring/review and use of the data must not go any further than the agreement.

[3] See below paragraphs 2.10

1.20. In the case of a looked after child, it would be good practice to refer to social media searches and checks in the care plan. If that is done, consent is not required for every search, provided the ambit of the activity is within that set out in the care plan.

1.21. If consent is refused, or would defeat the purpose of the monitoring, but the social worker considers that covert monitoring of an individual's social media is necessary for safeguarding purposes , RIPA authorisation should be obtained. If the purpose of the monitoring is not the detection or prevention of a serious crime, authorisation may be refused and an alternative legal basis for the monitoring must be established and specific legal advice should be obtained.

GDPR and Data Protection Act

1.22. Privacy rights are further protected by the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA), which require anyone processing the personal data of children to ensure that they have consent, or that there is another legal justification for the processing. The Information Commissioner's office (ICO) has the power to impose significant fines for breaches of the GDPR and the DPA, or the LA could be vulnerable to a damages claim. It is safest to assume that accessing social media for safeguarding purposes will include accessing 'special purposes' data which is information which is sensitive. This guidance is a very brief summary of the applicable principles as local authorities will have their own GDPR privacy policies in place.

1.23. Personal data includes any information about a living person, not just private information. Processing includes taking any action over the information – including accessing, storing, disseminating, recording, destroying.

1.24. Processing of social media or other data by those with safeguarding responsibilities will only be lawful if the data subject (or, in the case of a young child, the person or persons with parental responsibility in consultation with the child if the child is in care) has given their informed consent to that processing,

or if the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.[4] In the case of special category data (that is, information about sexual life or orientation, race, political opinion etc), then the processing will only be lawful if it is necessary for reasons of substantial public interest, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.[5]

1.25. In practice, this means that the processing of social media data for safeguarding purposes without consent needs to be justified by a proper public interest and to be as minimally intrusive as possible to fulfil the public interest purpose. Pursuing safeguarding concerns is a legitimate public interest purpose. If a social media search does not reveal any significant safeguarding issues, then the data should not be retained or disclosed and the public interest justification for the search must be recorded.

1.26. The 'data subject', that is the person whose information it is, has rights to information about the processing, including what information is being processed and to whom it has been disclosed. The data subject can also ask for information to be deleted or amended. These rights are limited where the purpose of the processing is social work. Further guidance and legal advice on how to respond to data protection requests from data subjects should be obtained if requests are made.

Privacy Claims

1.27. Breaches of the HRA or the DPA and the tort of misuse of private information could lead civil claims for damages, or an application for an injunction. A claim can be brought for misuse of private information or breach of the DPA six years after the misuse, whereas the right to sue for a breach of the HRA expires after one year. Material obtained in breach of the law may not be admissible in

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 6

[5] Ibid, Article 9

criminal proceedings though advice about the Family Court's approach to the admissibility of improperly obtained evidence is outside of the scope of this guidance.

1.28. There are some potential criminal offences in relation to accessing open source social media, although these are unlikely to apply in the safeguarding context. (See Appendix 1 – Protection from Harassment and DPA offences for further information)

1.29. Repeated systematic monitoring of a person's social media account is likely to be treated as directed surveillance in which case it is necessary to apply for authorisation under RIPA. It could be unlawful to monitor social media without such authorisation and any material obtained may not be admissible in court.[6]

2. Safeguarding obligations and obligations to court – specific issues for local authorities with statutory responsibilities

Reviewing social media for assessments

2.1. The duty of a LA to undertake assessments of need for children in its area is found at section 17 of The Children Act 1989 (Children Act). The July 2018 version of "Working Together to Safeguard Children" statutory guidance requires that when undertaking any assessment in respect of a child information should be gathered, recorded and checked systematically.[7]

2.2. The duty of a LA to make investigations necessary to properly inform decision making in respect of a child's welfare where there is a concern about harm is found at s47 of the Children Act 1989. S47(1) requires that a LA make *'such enquiries necessary to enable them to decide whether they should take any action to safeguard or promote the child's welfare'*. [8] Social workers should

[6] see paragraphs 3.2 below and Annex B

[7] HM Government, *Working Together to Safeguard Children - A guide to inter-agency working to safeguard and promote the welfare of childre*n (Published July 2018), pg 25, s.44

[8] The Children Act 1989, s 47(1)

when undertaking a s47 enquiry '*systematically gather information about the child and family's history'*, and *'seek advice and guidance as required and in line with local practice guidance*'.[9]

2.3. The position taken from the above is that when undertaking an assessment of a child's needs, whether under s17 or s47 Children Act, social workers involved are required to make enquiries that are necessary and proportionate to the issues raised in the referral received bearing in mind the aims of assessment under s17 and s47, and that enquiries and their outcomes should be recorded. A LA should not act in a way which is contrary to the law and therefore professionals exercising the functions of a LA need to ensure that their actions fall within the law set out in previous sections above. If queries arise as to whether a particular line of enquiry is necessary, proportionate, or lawful, advice and guidance should be sought.

2.4. If not rendered unlawful by other provisions [see above], viewing data which has been placed either by a child or a parent/relevant family member on social media without privacy conditions and therefore can be considered open source may be considered a proportionate and necessary enquiry for the public interest purpose of undertaking an assessment. However, repeat viewing of publicly available data sources without the knowledge of the target may constitute directed surveillance. This would apply to repeat viewing even of data not protected by privacy settings - see OSC Guidance and Codes of Practice.[10]

2.5. Even for proportionate, necessary and otherwise lawful one-off searches in the course of safeguarding assessment, an assessing social worker will need to give consideration to how they propose to access data not protected by privacy settings (for instance does a social worker propose to use their own personal account if data can only be accessed by a particular social media site's account holders), and advice may need to be sought about this on a case by case basis.

---

[9] N8, pgs 43-44

[10] Home Office, *Covert Surveillance and Property Interference Revised Code of Practice* (August 2018), para 3.15 (accessed 8 February 2019)

Setting up of a false identity is likely to be unlawful if it is for a covert purpose.[11]

2.6. If it is thought that repeated systematic searches of social media without the knowledge of the target are required in order to make enquiries to properly inform an assessment, guidance/legal advice should always be sought as this could be 'directed surveillance' and potentially unlawful without RIPA authorisation .. If there is a good public interest justification for such repeat viewing it may be lawful, but specific legal advice should always be obtained. Information considered necessary for the purpose of a properly informed assessment might otherwise possibly be obtained through seeking orders from the Family Court.

Role of LA in respect of Looked After Children and their use of social media

2.7. Local authorities most commonly come to look after children pursuant to consent of the parent (or of a child aged 16+) under s20 Children Act or through the making of a Interim Care Order or 'Full' Care Order under s38 Children Act and s31 Children Act respectively.

2.8. Where a child is looked after under s20 Children Act the LA does not gain parental responsibility for the child concerned. Parental responsibility remains with those who held it when the child became looked after.

2.9. Where a child is looked after under an Interim Care Order or a 'Full' Care Order the LA gains parental responsibility for the child, and the ability to determine the extent to which another person who holds parental responsibility (such as a parent) can exercise their parental responsibility - essentially allowing the LA to override the decisions (with a few exceptions) of a parent with parental responsibility - in circumstances where it is necessary to do so in order to safeguard or promote the welfare of the child.

[11] [11] Office of Surveillance Commissioners, *Procedures and Guidance* (published July 2016), pg 68, para 289.3

2.10. In either case s22 Children Act sets out the general duties of the LA in relation to the looked after child concerned. S22(3) sets out the LA's duty to safeguard and promote the looked after child's welfare. S22(4) requires that before making any decision relating to a child who they are looking after, the LA ascertain the wishes and feelings of the child and parent/anyone with parental responsibility as far as is reasonably practicable before the decision is made, and s22(5) requires that these wishes and feelings are given due consideration. LAs are required to prepare and maintain care and placement plans in respect of children in their care.

2.11. Relevant statutory guidance is available to LAs in the form of The Children Act 1989 guidance and regulations Volume 2: Care planning, placement, and case review (June 2015).[12] This provides guidance as to the implementation of the Care Planning, Placement and Case Review (England) Regulations 2010.

2.12. Regulation 5 sets out what a child's care plan should include. Of relevance to the question of social media use is that the care plan needs to include 'the arrangements made by [the LA] to meet [the child's] needs in relation to… emotional and behavioural development… and family and social relationships'.[13]

2.13. Regulation 9 and Schedule 2 to the regulations set out what a child's placement plan should include.[14] At 3.177 the Care Planning Guidance sets out that the child's placement plan should set out how the dad-to-day parenting tasks will be shared between the child's carer (for instance a foster carer) and the LA.[15]

2.14. At 3.206 the guidance suggests that decisions in respect of a looked after child are likely to fall into three broad categories. [16] Any sort of monitoring of a child's social media use is most likely to fit into the second category of 'routine but longer term decisions'. The guidance subsequently sets out at 3.207-3.210

[12] Department for Education, *The Children Act 1989 guidance and regulations Volume 2: care planning, placement and case review* (Published June 2015)

[13] The Care Planning, Placement and Case Review (England) Regulations 2010, Regulation 5

[14] Ibid, Regulation 9; Ibid, Schedule 2

[15] N13, pg 13, para 3.177

[16] Ibid, pg 94, para 3.206

that decisions in this category should be made through 'skilled partnership work involving the relevant people' - and so are not the sort to be delegated to the carer.[17]

2.15. The regulations themselves require that the placement plan makes clear who has the authority to make decisions in key areas of the child's day-to-day life including 'use of social media'.

2.16. With the above in mind, the general principles that should be applied to a question on whether and to what extent a LA can check/monitor a looked after child's social media data where the child is accommodated are:

2.16.1. If a child's social media usage has the potential to impact on the child's welfare, the LA should consider how the child's welfare can be safeguarded and promoted with regard to that social media usage. When considering whether and to what extent social media usage and content should be monitored, the LA should bear in mind all relevant considerations and the necessity and proportionality of any suggested measures.

2.16.2. When making any decision in respect of a looked after child, the wishes and feelings of the child and holders of parental responsibility should be sought if practicable. This principle will apply to decisions in respect of monitoring and/or restricting a child's use of social media.

2.16.3. Specific arrangements to meet a child's welfare needs in respect of their social media usage could in some cases appropriately be recorded in the child's care plan, potentially in those sections of the care plan which address the LA's arrangements to meet the child's needs in relation to 'emotional and behavioural development' and 'family and social relationships'. If the care plan includes arrangements for systematic monitoring of publicly available social media accounts or internet searches, the monitoring would not be covert and so no RIPA

[17] Ibid, pgs 94-95. paras 3.207-3.210

authorisation would be needed. The monitoring would still involve potentially private information and so should be for a proper public interest purpose (e.g. necessary for protecting the child) and proportionate (as unintrusive as possible to fulfil the purpose).

2.16.4. The seat of responsibility for decision-making in respect of the child's social media usage should be confirmed in the child's placement plan, and it is unlikely that decisions in respect of monitoring social media activity or usage should be left to the child's carer.

2.16.5. Where a LA is accommodating a child under s20 Children Act, it will not hold parental responsibility for the child concerned or the ability to limit the decision-making of those who hold parental responsibility for a child under the age of 16. Decisions and plans for the monitoring of social media usage and content should be agreed with those who hold parental responsibility if possible. If the child is 16+, the child's agreement should be sought. Further advice and guidance should be sought if agreement is not possible or if it is given but subsequently withdrawn.

2.16.6. Where a LA holds an interim or final care order in respect of a child, this will mean that it holds parental responsibility for the child which it will usually share with others (for example parents) who also hold parental responsibility. Decisions and plans for the monitoring of social media usage and content should be agreed with the other holders of parental responsibility if possible, unless the LA has decided not to involve the parents for instance because it is felt that this is necessary in order to safeguard the child. If agreement is not possible consideration may be given to whether the LA can appropriately exercise its power to enforce its own decision on what is best for the child over the parents' objections using its power under s33 Children Act - in such a case further advice and guidance should be sought.

3. RIPA and potential criminal offences (See Annex A and B for additional information)

3.1. If direct surveillance is contemplated the consent of the person being monitored should be obtained. If this is not practicable or defeats the purpose and online monitoring is conducted covertly for the purpose of a specific investigation and is likely to result in the obtaining of private information about a person or group, RIPA authorisation for directed surveillance should be considered and may well be required.[18] Direct surveillance would include the systematic monitoring of an individual's online social media without their knowledge, such as regular and repeat access to a Facebook account or Instagram account, even it is publicly available without privacy settings.

3.2. In order for an LA to obtain RIPA authorisation the purpose of the directed surveillance must be:

- to detect or prevent crime;
- A specific crime must be investigated;
- The crime being investigated must carry a custodial sentence of at least 6 months;
- The surveillance must be necessary and proportionate in the circumstances.

3.3. The core function of a LA in this context is to safeguard, not to detect or prevent crime. However, there are rare cases where this may overlap (and the OSC guidance does envisage this, see Appendix B). In practice, RIPA authorisation will rarely be granted (for direct surveillance) because, if a specific crime that attracts a sentence of over 6 months is suspected, usually this matter would be referred to the police to carry out whatever investigations are required as this is not a core function of the LA. However, if it is felt there is a need to covertly systematically monitor and track social media, this would require RIPA authorisation and all the above requirements would have to be met on an application to the court.

[18] N10, pg 18-19 para 3.10-3.15

3.4. If the monitoring is not for the purposes of detecting or preventing crime but for a pure safeguarding purpose, the monitoring is outside the ambit of RIPA. A proper public interest purpose or Article 8(2) justification must be established.[19] Specific legal advice will be required in order to establish a lawful basis for direct surveillance and a court order may be required.

3.5. Single viewing of social media to establish, for example, if the subject is in a relationship when they have stated they are not, would not come within the meaning of direct surveillance. But the LA needs to be aware that repeatedly accessing, collecting and recording social media or other open source information about a particular person or group, even if it is publicly available online, without that person's knowledge or consent would be classed as directed surveillance and authorisation should be considered. It is unlikely that RIPA authorisation would be granted for that purpose. Evidence obtained without such authorisation, may not be admissible in a criminal court and could lead to a damages claim under the HRA. It would also destroy all trust between the LA and the subject. All this being the case, anything over a single search and viewing of publicly available social media contact without adequate consent or without the knowledge of the subject is likely to be inadvisable even if otherwise thought to be necessary and proportionate to inform a safeguarding assessment, and specific legal advice should be sought if it is proposed.

3.6. If it is believed direct surveillance is required to prevent or detect a crime carrying a sentence of over 6 months, usually this should be referred to the police. See Annex B for detailed information about RIPA.

3.7. In rare circumstances, if a LA or their employees monitor social media or obtain and retain personal information without consent this could potentially amount to a criminal offence under the Protection from Harassment Act 1997 or the DPA 2018. Providing there is a proper public interest purpose in what is being done and what has been done is reasonable in the circumstances, it is highly unlikely that an offence has been committed. . See Annex A for additional information.

[19] See para 1.5

Summary advice

Green light – steps which may be taken where there is a safeguarding concern

- **A single Google search and/or social media search on the name of the target and review of information which is responsive to those targets without keeping the information obtained on file**
- **Where the search involves children as the target of the search, be aware that the information is likely to be private and keep a record of the justification for the search and the outcome (the public interest in reviewing social media).**
- **Record that a search have taken place without any concerns being identified and date of search (without keeping a record of the information obtained unless necessary)**
- **Searches and monitoring for purposes of assessment/care where there is properly informed consent and that the need for ongoing monitoring is kept under review with regard for necessity and proportionality.**
- **In all cases, searches should only be carried out where necessary**

Orange light – steps which may be taken but exercise caution and take additional legal advice if necessary

- **storing information and sensitive information obtained from childrens' social media accounts or online searches -sometimes information may be 'public' but private and sensitive and shouldn't be accessed or stored without a specific justification. Social media of children should usually be treated as private information and a specific public interest justification for retaining and storing the information should be recorded.**
- **disclosing information obtained as a result of social media searches – be careful that disclosure is for a safeguarding purpose (e.g. to police or social workers in another area or a teacher), is no more than necessary to fulfil that purpose and that the purpose of the disclosure is recorded in the file**
- **monitoring or restricting a child's social media use should be done in conjunction with the person who has parental responsibility if possible, and**

recorded in the care plan and with appropriate consultation with the child concerned in the case of looked after children

- **single or occasional repeat viewing of public domain social media may be undertaken, but once this becomes repeat monitoring or surveillance, it is likely to be unlawful without RIPA authorisation and/or consent of those with parental responsibility or the child, or order from family court. Refer to police or to legal team for further advice if concerns remain.**

Red light – never do without specific legal advice

- **Searches of social media where no safeguarding reason.**
- **Assuming a false identity to befriend someone and access their social media**
- **Befriending someone in your own name in order to monitor their social media accounts**
- **Repeated monitoring, collecting and recording information about a particular person or group, including surveillance of social media accounts without the knowledge of the target, even where the social media account is public.**
- **Retaining records of the above**
- **Disclosing private information to others outside safeguarding roles**

Annex A

Criminal offences

Potential Criminal matters regarding online monitoring of open source material.

The Protection from Harassment Act 1997[20] (as amended) sets out the offences of harassment and stalking and potential defences.

Those sections relevant to covert online monitoring of an individual's social media or private activities online using open sources or internet searches are s1 and s2A of the Protection of Harassment Act 1977.

This would come under stalking (see section 2A below for full summary).

This Act prohibits stalking if it amounts to **a course of conduct** and **harassment** of an individual.[21]

Examples of stalking that could amount to harassment provided within the Act are:

a) following a person,
b) contacting, or attempting to contact, a person by any means,
c) publishing any statement or other material—
    (i) relating or purporting to relate to a person, or
    (ii) purporting to originate from a person,
d) monitoring the use by a person of the internet, email or any other form of electronic communication,
e) loitering in any place (whether public or private),
f) interfering with any property in the possession of a person,
g) watching or spying on a person.[22]

(d) and (g) are most likely to apply to monitoring of an individual's social media and online activity. The activity would have to take place more than once and occur relatively closely in time to amount to a "course of conduct" and thus a potential offence. The monitoring does not have to be covert to amount to an offence if it causes alarm and distress to the subject.

[20] Protection from Harassment Act 1997
[21] Ibid, s 1(1)
[22] Ibid, s 2A(3)

The individual carrying out the activity would have to know or ought to know that it would amount to harassment/stalking and the conduct would have to be unacceptable and oppressive to meet the criminal standard.

The defences that apply to the conduct envisaged within the s2A stalking offence are:

- that it was pursued for the purpose of preventing or detecting crime;
- that it was pursued under any enactment or rule of law;
- that it was reasonable in the particular circumstances.[23]

If a decision is made to view an individual's online activity or their social media to assist with an assessment of compliance with court orders or agreements, or for safeguarding purposes, this is likely to be considered reasonable, but Article 8 should always be considered. If monitoring is necessary for a safeguarding purpose or there is another good public interest reason for reviewing the material, then there will be no criminal liability.

Irregular viewing is unlikely to fall foul of the PHA.

Local authorities are not permitted to intercept the content of any person's communications and it is an offence to do so without lawful authority.

Offence under the Data Protection Act 2018[24]

S.170 DPA 2018 creates an offence to unlawfully obtain and then retain personal data without the consent of the controller. In the case of personal data posted online (e.g. online forums or social media), the data controller will either be the person posting the personal information or the organisation running the site depending on their terms and conditions for users.[25]

For the LA to monitor and in doing so record personal information of individuals that is available on social media without the consent of the individual or the site, there is a potential offence under s170 DPA.

It is a defence if the person charged can prove that the obtaining / retaining of the data was:

- necessary for the purposes of preventing or detecting crime,

[23] Ibid s 4(3)
[24] Data Protection Act 2018
[25] Ibid, s 179

- was required or authorised by an enactment, by a rule of law or by the order of a court or tribunal, or
- in the particular circumstances, was justified as being in the public interest.
- Or that they reasonably believed that the obtaining/retaining was justified as being in the public interest.[26]

In practice, there is an extremely low likelihood of criminal liability in relation to a social worker or person with safeguarding responsibility obtaining and retaining data for safeguarding purposes. But it should be noted that if any social media is obtained or retained for other purposes, there could be. For example, if a social worker obtained photographs of a child practicing dance moves from a child's social media account for safeguarding purposes, but then kept them to show her nieces the dance moves, that could be an offence.

For confirmation of the role of LA and use of RIPA see the following Home Office Guidance:

Protection of Freedoms Act 2012 (PFA 2012)– changes to provisions under the Regulation of Investigatory Powers Act 2000 (RIPA)[27]

Home Office guidance to local authorities in England and Wales on the judicial approval process for RIPA and the crime threshold for directed surveillance.

[26] Ibid, s170 (2-3)

[27] Home Office, *Protection of Freedoms Act 2012 – changes to provisions under the Regulation of Investigatory Powers Act 2000 (RIPA)* (Published October 2012)

Annex B

Regulation of Investigatory Powers Act (RIPA) 2000[28]

Preamble and Government Guidance:

1. RIPA was designed to regulate the use of investigatory powers and to satisfy the requirements of the ECHR on its incorporation into UK law by the Human Rights Act 1998.

2. RIPA sets out a regulatory framework for the use of covert investigatory techniques by public authorities. RIPA does not provide any powers to carry out covert activities.

3. RIPA regulates the use of a number of covert investigatory techniques, those available to local authorities are:

   i) the acquisition and disclosure of communications data (such as telephone billing information or subscriber details);

   ii) directed surveillance (covert surveillance of individuals in public places or monitoring of open source online activity); and

   iii) covert human intelligence sources ("CHIS") (such as the deployment of undercover officers)

4. For the purpose of this guidance we are only concerned with direct surveillance as defined by s26 (2)-(6), namely:

   It is covert but not intrusive and is undertaken:

   a) for the purposes of a specific investigation or a specific operation;
   b) likely to result in the obtaining of private information about a person and
   c) otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under this Part to be sought for the carrying out of the surveillance.

5. "Private information" includes any information relating to an individual's private or family life.

[28] Regulation of Investigatory Powers Act (RIPA) 2000

6. Directed surveillance is covert surveillance in places other than residential premises or private vehicles. Local authorities cannot carry out intrusive surveillance (covert surveillance in residential remises and private vehicles) within the RIPA framework.

7. S28 (3) (b) RIPA provides that authorisation for directed surveillance can only be granted by those designated to do so if :

   i) it is necessary for the purpose of preventing or detecting crime or of preventing disorder;

   ii) and that crime carries a maximum term of imprisonment of 6 months or more (Child cruelty, neglect, violent and sexual offences would carry a sentence of over 6 months. Common assault does not.)

8. Use of these techniques has to be authorised internally by an authorising officer or a designated person. They can only be used where necessary and proportionate.

9. This involves balancing the intrusiveness of the activity on the target and others affected by it against the need for the activity to meet the objectives. Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation.

10. The activity will not be proportionate if it is excessive in the circumstances of the case or if the information sought could be easily obtained by less intrusive means. The seriousness of the allegations being investigated will impact on the proportionality and necessity test. All cases are fact specific.The Chief Surveillance Commissioner (CSC) is responsible for overseeing local authorities' use of directed surveillance.

12. In March 2017 the Commissioner wrote to all local authorities in the following terms:

"It has become steadily more apparent that a number of officers working for public authorities, particularly those with responsibilities for the care of children and vulnerable adults have started to use the [social media and internet] sites, acting in good faith and on their own initiative. ***RIPA issues do not normally arise at the start of any investigation which involves accessing "open source" material, but what may begin as a lawful overt investigation can drift into covert surveillance which falls within the legislation. Although the investigation of crime is not normally a "core function" of the Council, the protection of children and vulnerable adults certainly is, and any***

continuing and deeper study of the social media site in question would only be justified by the exercise of that protective function.

These are complex legislative provisions, and without appropriate training and awareness council officers cannot be expected to appreciate and apply them. They may therefore act unlawfully. Ignorance would provide no defence to them personally, nor to the Council for which they were working."[29]

13. It is important to note that Local Authorities cannot apply for RIPA authorisation for safeguarding per se. Their core function is the protection of children and vulnerable adults, not the investigation of crime. This is generally a matter for the police. However, if, in order to meet that core function it is necessary and proportionate to monitor social media and the internet, repeated and targeted monitoring of social media may amount to direct surveillance and RIPA authorisation would be required. Any covert surveillance should be demonstrably necessary and proportionate to the achievement of the legitimate aim (to protect children and vulnerable adults) through the investigation of a criminal offence.

14. The Home Office Guidance, comments by the CSC in his annual report and the judgment in *Re E & N (No 2)* do not, in my view, properly follow the legislation.[30] The PFA 2012 amended RIPA 2000 in order to limit the ability of LA's to carry out direct surveillance to prevent or detect crime and clearly placed it in the investigative context. The CSC conflates the investigation of a crime with the protection of children and vulnerable adults[1]. However, as is clear from *E & N 2017 (No2),* the courts are interpreting such activity as coming within the RIPA framework and in *E & N* the Judge clearly took the view that authorisation would have been granted if it had been applied for. But, if a LA was investigating a less serious crime of ABH or relatively minor neglect which attract sentences of 6 months or more, authorisation may be less likely

15. In terms of LSB Guidance , it is essential that the LA always has in mind that direct surveillance is only permissible to detect/prevent crime (an offence that attracts a sentence of over 6 months), but in a safeguarding context. Home Office Guidance states that directed surveillance will be authorised against a specific offence which meets the

[29] Letter from the Rt Hon Lord Judge (aka Chief Surveillance Commissioner), dated 20 March 2017
[30] *Re E & N (No 2)* [2017], Case Nos. RG16C00639 & RG17C00104

threshold.[31] It is clear from the Home Office Guidance that directed surveillance is only permissible if a specific criminal offence is being investigated.[32]

16. The CSC has made it clear that monitoring and use of the internet and social networking sites may fall within the definition of covert directed surveillance. This is likely to result in the breaching of an individual's Article 8 rights under the Human Rights Act (the right to privacy) and will require RIPA authorisation. A lack of privacy settings does not mean an individual has consented to their online activity being observed or monitored.

17. The authorised surveillance is proportionate to what it is expected can be achieved by it. This involves balancing the intrusiveness of the activity on the target and others who might be affected by it against the need for the activity in operational terms. The activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair.

18. If any evidence obtained by directed surveillance is to be relied on in proceedings, all reasonable steps should be taken to verify the accuracy of that information

[31] N26, pg 9, para 24
[32] Ibid, pg 8, para 23