APPENDIX 4

Social Media Investigations/Internet Research Policy

JUNE 2021

Contents

BACKGROUND OF POLICY

Most of the information available on the internet is available to any person with internet access. Such information is widely known as open source information. Online open source research is widely regarded as the collection, evaluation and analysis of material from online sources available to the public, whether by payment or otherwise to use as intelligence and evidence.

The use of online open source internet and social media research techniques has become a productive method of obtaining information to assist Tameside Metropolitan Borough Council with its regulatory and enforcement functions. It can also assist with other functions such as service delivery issues and debt recovery. However, the use of the internet and social media is constantly evolving and with it the risks, particularly regarding breaches of privacy under Article 8 Human Rights Act (HRA) and other operational risks.

Tameside Metropolitan Borough Council is a Public Authority in law under the Human Rights Act 1998, and as such, the staff of the authority must always work within this legislation. This applies to research on the internet. Just because it may seem easier to carry out internet research does not mean that it should take place without justification.

LEGAL FRAMEWORK

This procedure is a restricted document for use by Tameside Metropolitan Borough Council staff only. It should not be published or distributed or disclosed under Freedom of Information Requests. It is relevant for Criminal and Civil Proceedings.

This procedure establishes Tameside Metropolitan Borough Council corporate standards and instructions, which will ensure that all online research and investigations are conducted lawfully and ethically to reduce risk. It provides guidance to all staff, when they are engaged in their official capacity of the implications and legislative/best practice framework associated with online internet and social media research. It will also ensure that the activity undertaken, and any evidence obtained will stand scrutiny.

The aim is to ensure that information gathering, investigations or surveillance involving the use of Social Media are conducted lawfully and correctly in accordance with an individual's human right and with due consideration of relevant legislation and Council policies including:

- Human Rights Act 1988 (HRA)
- European Convention on Human Rights (ECHR)
- Data Protection Legislation (Data Protection Act 2018 (DPA)
- Regulation of Investigatory Powers Act 2000 (RIPA) and
- together with the published codes of practice from the Home Office, Investigatory Powers Commissioner's Office (IPCO), formerly the Office of Surveillance Commissioners (OSC), and the Information Commissioner's Office.
- Tameside Metropolitan Borough Council Policy Social Media Use Responsible Conduct Policy. May 2018.

This policy and procedure should also be read in conjunction with the Council's Regulation of Investigatory Powers Act 2000 (RIPA) policies and procedures, as well as the statutory codes of practice issued by the Secretary of State and the Investigatory Powers Commissioner's Office (IPCO) Guidance. Should there be any queries, advice can be sought from Legal Services. Where activity meets the RIPA criteria, the RIPA policy and procedures must be followed.

Not adhering to policy and procedures could result in members of staff being dealt with through the Council's disciplinary procedure.

Use of Social Media in investigations refers to any instance where an officer accesses Social Media

as described to formally or informally gather evidence for any kind of investigation.

WHAT IS MEANT BY SOCIAL MEDIA

Social Media has become a significant part of many people's lives. By its very nature, Social Media accumulates a sizable amount of information about a person's life, from daily routines to specific events. Their accessibility on mobile devices can also mean that a person's precise location at a given time may also be recorded whenever they interact with a form of Social Media on their devices. All of this means that incredibly detailed information can be obtained about a person and their activities.

Social Media will always be a web-based service that allows individuals and businesses to construct a public or semi-public profile. Social Media can be very diverse, but 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
- Hosting capabilities allowing users to post audio, photographs and/or video content that is viewable by others.

Social Media can include community based web sites, online discussions forums, chatrooms and other social spaces online as well.

Current examples of the Social Media, and therefore the most likely to be of use when conducting investigations into alleged offences, include:

- Facebook
- Twitter
- Instagram
- LinkedIn
- Pintrest
- Tumblr
- Reddit
- Flickr
- Google+

Please note that this is not an exhaustive list.

Social media sites have allowed individuals, businesses and organisations to easily communicate between each other, serving as a useful tool to keep in touch and interact on what can be a real time basis.

People or groups can instantaneously share information, coordinate events and provide updates that are of interest to their friends, family or customer base.

Social media sites can also serve as a platform for individuals or groups to express their opinions and social, political and religious beliefs to give just a few common examples.

It is also possible to share photographs or videos with others and where privacy settlings allow, to share the posts of other people not necessarily connected with the original person.

UTILISING SOCIAL MEDIA WITHIN AN INVESTIGATION

Social Media can therefore be a very useful tool when investigating alleged offences with a view to

bringing a prosecution in the courts. The use of information gathered from the various different forms of Social Media available can go some way to proving or disproving such things as whether a statement made by a defendant, or an allegation made by a complainant, is truthful or not. However, there is a danger that the use of Social Media can be abused, which would have an adverse effect, damaging potential prosecutions and even leave the Council open to complaints or criminal charges itself.

Public Authorities must ensure that any interference with Article 8 is:

- Necessary for a specific and legitimate objective –such as preventing or detecting crime;
- Proportionate to the objective in question;
- In accordance with the law.

Whenever you are using the internet to gather intelligence or evidence you must consider whether you are likely to interfere with a person's private and family life and, if so, whether you should seek authorisation under the Regulation of Investigatory (RIPA) for your conduct.

It is also essential to consider the effect of any collateral intrusion on the private and family life of other people not directly connected with the subject of the research or investigation.

Case by case judgement is vital when researching or investigating online. There are some considerations and standards to apply when using such sites, which this policy covers.

PRIVACY SETTINGS

The majority of Social Media services will allow its users to decide who can view their activity, and to what degree, through the use of privacy settings. Whilst some users are happy or indifferent about who is able to view their information, others prefer to maintain a level of privacy.

The information publicly available is known as an individual's public profile.

Depending on their intentions, many users will purposely use Social Media with no privacy setting applied whatsoever. This could be due to the fact that they are actively promoting something, such as a business or event, and therefore require as many people as possible to be able to view their Social Media profile at all times; others may do so for reasons of self-promotion or even vanity. Furthermore there may be a lack of awareness of what others can see and how to protect their privacy.

Those individuals with public profiles who operate on Social Media without any, or only limited, forms of privacy settings being activated do so at their own risk. Often, Social Media sites will advise its users through its terms and conditions of the implications of not activating privacy controls, namely that all content they publish or share will be viewable by everyone, including sometimes people who, themselves, do not have an account with that provider.

Whilst the content or information shared by individuals on Social Media remains the property of that individual, it is nonetheless considered to be in the public domain. Publishing content or information using a public, rather than a private setting, means that the individual publishing it is allowing everyone to access and use that information, and to associate it with them.

The opposite of a public profile is a private profile. Some users of Social Media will not wish for their content, information or interactions to be viewable to anyone outside of a very small number of people, if any. In these instances, users will normally set a level of privacy on their Social Media profiles that reflects what they are comfortable with being made available, meaning that, for example, only friends, family and other pre-approved users are able to view their content or make contact with them through that site.

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).

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, for example:

Person A publicises on their private Social Media page that they intend to throw a party, at which they will be selling alcohol and providing other forms of licensable activities, despite not having a licence from the Council to do so. Person B, who “follows” Person A’s Social Media page, re-publishes this information on their public Social Media page. The information on Person A’s profile cannot be used, however, the same information on Person B’s profile, can.

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. Multiple and systematic viewing of the information would therefore require a RIPA authorisation.

RISK

Officers should be made aware that any activity carried out over the internet leaves a trace or footprint which can identify the device used, and, in some circumstances, the individual carrying out the activity. Unless the activity is conducted lawfully, Tameside Metropolitan Borough Council may face legal proceedings for breaching the Article 8 right of the person who is the subject of the research or investigation. There are also legal and reputational risks in failing to handle private information in accordance with GDPR and the DPA.

General routine ‘one-off’ social media enquiries will rarely pose a risk as they will be carried out in an open official capacity, as opposed to a covert capacity.

Using trained staff to undertake certain online research will reduce risks. The use of untrained staff will be a risk-based decision by the departmental managers based on the skills and experience of the individual undertaking the research and the nature and level of the research required.

NECESSITY/JUSTIFICATION

To justify the research or investigation, there must be a clear lawful reason, and it must be necessary. Therefore, the reason for the research, such as, the criminal conduct that it is aimed to prevent or detect must be identified and clearly described. This should be documented with clear objectives. Should the research or investigation fall within the scope of RIPA (i.e. by amounting to ‘directed surveillance, the activity must not proceed without prior authorisation in accordance with RIPA procedures, including the need to show necessity on specified statutory grounds.

PROPORTIONALITY

Proportionality involves balancing the intrusiveness of the research on the subject and other innocent third parties who might be affected by it (collateral intrusion) against the need for the activity in operational terms. This requires an evaluation of the benefit to carrying out the activity relative to the seriousness of the suspected conduct under research or investigation, and of the expected benefit of the activity versus the privacy intrusion. 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.

Where online activity amounts to directed surveillance, part of the application for prior authorisation requires the applicant to demonstrate proportionality to the standard required by RIPA and its relevant Code of Practice.

PRIVATE INFORMATION

RIPA provides that 'private information' includes any information relating to a person's private or family life. Private information should be taken generally to include any aspect of a person's private or personal relationship with others, including family and professional or business relationships.

Prior to, and during any research, officers must take into account the privacy issues regarding any person associated with the research. Where an officer considers that research may interfere with a person's right to privacy, he/she must obtain authorisation from the line manager before proceeding. The line manager must be satisfied the proposed interference is lawful, before consenting to its use.

COLLATERAL INTRUSION

Collateral intrusion is the interference with the private and family life of persons who are not the intended subjects of the research. Measures should be taken, wherever practicable, to avoid or minimise interference with the private and family life of those who are not the intended subjects. Where such collateral intrusion is unavoidable, the activities may still be authorised providing it is considered proportionate to what is sought to be achieved. The same proportionality tests apply to anticipated collateral intrusion as to intrusion into the privacy of the intended subject of the surveillance.

Any collateral intrusion should be kept to the minimum necessary to achieve the specific objectives of the research.

All types of research should therefore include an assessment of the risk of any collateral intrusion, and details of any measures taken to limit and manage the intrusion. This will form part of the procedure if RIPA is engaged.

COVERT HUMAN INTELLIGENCE SOURCE (CHIS)

There is a considerable amount of information on the internet associated with illegal activity such as, unlicensed operators and fly-tipping offenders advertising through social media. To successfully obtain sufficient evidence and intelligence, it may be necessary to covertly communicate with suspects online. This is likely to require a CHIS authorisation.

The guidance relating to online covert CHIS activity is in the RIPA CHIS Codes of Practice. The below information is taken from the codes.

DEFINITION OF A COVERT HUMAN INTELLIGENCE SOURCE (CHIS)

A CHIS is a person who establishes or maintains a personal or other relationship with a person for the purpose of covertly using the relationship to obtain information, or provide access to any information to another person, or covertly discloses information.

A purpose is covert, if and only if, the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.

Any manipulation of a relationship by a public authority (e.g. one party having a covert purpose on behalf of a public authority) is likely to engage Article 8, regardless of whether or not the public authority intends to acquire private information.

The lawful criteria for CHIS is prevention and detection of crime and prevention of disorder and the offence does not have to have a sentence of 6 months imprisonment. If the enquiry was not for this purpose such as safeguarding or a disciplinary issue it would amount to CHIS activity outside of RIPA which should be authorised under that procedure.

This would equally apply to using a member of the public as it would to a member of Tameside Metropolitan Borough Council staff making the contact. The Codes of Practice at 4.12 state "where someone, such as an employee or member of the public, is tasked by a public authority to use an internet profile to establish or maintain a relationship with a subject of interest for a covert purpose, or otherwise undertakes such activity on behalf of the public authority, in order to obtain or provide access to information, a CHIS authorisation is likely to be required. For example:

- An investigator using the internet to engage with a subject of interest.

- Directing a member of the public (such as a CHIS) to use their own or another internet profile to establish or maintain a relationship with a subject of interest for a covert purpose.

- Joining chat rooms with a view to interacting with a criminal group in order to obtain information about their criminal activities.

WHAT IS PERMITTED UNDER THIS POLICY

Whether or not Social Media can be used in the course of investigation an offence, or potential offence, will depend on a number of things, including if the suspect has a Social Media presence at all. Investigating officers should also utilise overt traditional techniques and not place too high an emphasis on Social Media. For example, the lack of information on a social media profile should not be taken as evidence that something is or isn't true.

Using social media for investigatory purposes, under statutory powers or otherwise, will meet the definition of "directed surveillance under RIPA 2000,"if it is:

1. covert;
2. likely to reveal private information; and
3. done with some regularity

The primary consideration is the privacy settings and whether the person being monitored has a public or private profile as above.

The general observation duties of many law enforcement officers and other public authorities do not require RIPA authorisation, whether covert or overt. Such general observation duties frequently form part of the legislative functions of public authorities, as opposed to the pre-planned surveillance of a specific person or group of people. General observation duties may include monitoring of publicly accessible areas of the internet in circumstances where it is not part of a specific investigation or operation. (3.33 Aug 2018 RIPA Codes of Practice)

COUNCIL POLICY REFLECTED ACROSS DIRECTORATES

Tameside Metropolitan Borough Council's policy is that these types of enquiries MUST consist of attributable, overt, initial non-repeated research. This includes any research that is intended to identify themes, trends, possible indicators of criminality or other factors that may influence operational strategies. Some examples are shown below

- viewing publically available postings or websites where the person viewing does not have to register a profile, answer a question, or enter any significant correspondence in order to view. e.g a typical trader's website.

- Initial research to proactively identify how many persons are advertising waste collection via social media to tackle illegal waste (fly-tipping).

- Initial enquiries to corroborate a complaint of a regulatory nature.
- Enquires relating to safeguarding issues.
- Initial enquiries to establish whether a suspect in an enforcement investigation has an online presence to assess whether there is intelligence or evidence available
- Initial enquiries to trace a debtor.

General routine enquiries will not normally engage the RIPA procedure as they are open and transparent and not normally repeated. There will be a low expectation of privacy and no RIPA authorisation would normally be required to view or record these pages. They also need to be carried out using Tameside Metropolitan Borough Council networked computers via open search engines such as Google.

TEAMS WITHIN REGULATORY SERVICES, namely Trading Standards, Licensing, Exchequer and Environmental Health are responsible for ensuring compliance with a wide range of criminal legislation. Many businesses now operate solely on social media sites now, and it is therefore necessary, in order to protect the public and to ensure compliance with legislation, that officers can use social media. Some examples where the use of social media is necessary and proportionate is to identify and establish evidence of sellers of counterfeit goods; illicit tobacco; and unlicensed tattooists, skin piercers and dog breeders, business grants/owners.

CHILDREN AND FAMILIES: Children's Social Care can use a range of methods when attempting to locate / contact absent or estranged parents in order to provide notice of care proceedings. Judicial bodies have highlighted the role that social media sites can play in ensuring parents know about care proceedings (Justice Holman, February 2017).

Social workers can use Facebook to search for missing parents, says judge (communitycare.co.uk)

Similarly, use is appropriate where there are concerns around safeguarding, exploitation, or children missing from home.

https://www.basw.co.uk/system/files/resources/Social%20Media%20Policy.pdf#:~:text=Social%20media%20is%20being%20used%20in%20safeguarding%20investigations,practice%20and%20legislation%20to%20protect%20and%20empower%20children.

Education Services can also use social media to locate children who are missing from education. There has been much debate nationally on the use of such platforms in contacting children, young people and families and gathering evidence for the purpose of assessment or proceedings. Please see appendix B to this policy.

ADULT HEALTH AND SOCIAL CARE:

Support and Safeguarding teams may try to locate vulnerable adults or need to identify / request contact with guardians or care givers.

Adult Social care teams can use a range of methods when attempting to locate / contact absent vulnerable adults in order to ensure they are safe. Similarly, use is appropriate where there are concerns around safeguarding or exploitation. There is lots of evidence of the benefits of using social media in social care as long as the service works within its organisational guidelines.
Depending upon the purpose of the business, these accounts can be 'overt' (an open public page) or 'covert' (hidden from public view).

When using social media, the approach taken by all employees needs to be proportionate, necessary and have a recognised legitimate aim that protects the individual's privacy rights and meets the following legislative requirements:

- The Data Protection Act 2018 and GDPR.
- Article 8 of the Human Rights Act (Individual's right to privacy).
- Regulation of Investigatory Powers Act, 2000.

As stated, the systematic accessing or consistent monitoring of an individual's /business's internet and social networking site may potentially fall within the definition of covert directed surveillance, which would require authorisation to be sought from a Magistrates Court. Failure to seek authorisation when necessary could result in the Council breaching an individual's right to privacy (Article 8 of the Human Rights Act). It is therefore important that officers follow this policy and seek additional advice if necessary,in respect of The Regulation of Investigatory Powers Act when considering accessing internet and social networking sites. Please see appendix B to this policy.

ONE- OFF VISITS

A distinction is made between one-off and repeated visits to an individual's Social Media profile.

One-off visits, or otherwise infrequent visits spread out over time, would not be considered "directed surveillance" for the purposes of RIPA. Repeated or frequent visits however may cross over into becoming "directed surveillance" requiring RIPA authorisation.

A person's Social Media profile should not be routinely monitored e.g on an hourly, daily or weekly basis, in search of updates as this would require RIPA authorisation.

A "one-off" is an on-line visit of a social media platform to gather information that is publically available. A log must be maintained within the investigation file detailing the date and time of each visit and a brief note of the information gained, which is pre-authorised by the officer's line manager.

Each single viewing of an individual's social media site must be recorded on the log.

For any surveillance that is more than a "one-off", those involved should consider whether to seek RIPA authorisation. Officers should consider the parallel situation: live, covert observation of a person in public places. If an authorisation would be required in the real world, one would also be required in the virtual world. Continued covert visits are likely to be unjustifiable without formal consideration under RIPA.

Prior to commencing general routine enquiries on the internet, Line Manager (Service Unit Manager- minimum level) approval will be required. This should be clearly documented within the case file notes preferably by using the form provided at Appendix A.

WHAT IS NOT PERMITTED UNDER THIS POLICY

Council officers should **NOT** attempt to circumvent privacy settings and view an individual's information on multiple occasions unless authorisation has been sought under RIPA. Such attempts may include, but are not limited to;

- sending "friend", 'like', 'create and/or send posts' or "follow" requests to the individual and/or company;
- setting up or using bogus Social Media profiles in an attempt to gain access to the
- individual's and/or company's private profile;
- contacting the individual and/or company through any form of instant messaging or chat function requesting
- access or information;
- asking family, friends, colleagues or any other third party to gain access on their behalf,
- or otherwise using the Social Media accounts of such people to gain access; and /or
- using any other deceptive or misleading method

- **repeated viewing (2 times or more within a 28 day period within the same department) of 'open source' information is NOT PERMITTED and requires a RIPA authorisation.**

USE OF OFFICIAL ORGANISATION / DEPARTMENTAL SOCIAL MEDIA ACCOUNTS

Social media accounts used for investigation purposes and/or linked research must only be accessed on devices belonging to the council. When conducting internet enquiries or investigations, these must be carried out through a dedicated Council-wide Investigations/research Social Media account for the specific purpose of carrying out an investigation and/research, through genuine open source techniques and openly available search engines such as Google (open site)

Officers are **NOT** permitted to create additional departmental social media accounts and/or their own personal social media accounts for the purposes of investigations/gathering information. This is because it is impossible to effectively monitor and control due to the potential number of users and associated risks of officers potentially acting unlawfully. There are also implications for the officers, as they are leaving audit trails,that are inappropriate. As a result, it is likely to leave the council facing liability issues over potential breaches of privacy under the HRA or other legislation such as RIPA and the GDPR.

CAPTURING EVIDENCE

Once content available from an individual's social media profile has been identified as being relevant to the investigation being undertaken, it needs to be recorded and captured for the purposes of producing as evidence at any potential prosecution. Depending on the nature of the evidence, there are a number of ways in which this may be done.

Where evidence takes the form of a readable or otherwise observable content, such as text, status updates or photographs, it is acceptable for this to be copied directly from the site, or captured via a screenshot, onto a hard drive or some other form of storage device, and subsequently printed to a hard copy. The hard copy evidence should then be exhibited to a suitably prepared witness statement in the normal way.

Where evidence takes the form of audio or video content then efforts should be made to download the content to the authorised location on the Council's storage systems. This should be agreed by each Service and IT Services. In the event that material needs to be copied to a USB pen drive please refer to the Removable media please on the Intranet. The relevant Council data retention periods must also be adhered to.

When capturing evidence from an individual's public social media profile, steps should be taken to ensure that all relevant aspects of that evidence are recorded effectively. For example, when taking a screenshot of a person's social media profile, the officer doing so should make sure that the time and date are visible on the screenshot in order to prove when the evidence was captured. Likewise, if the evidence being captured is a specific status update or post published on the person's profile, steps should be taken to make sure that the date and time of that status update or post is visible within the screenshot. Without this information, the effectiveness of the evidence is potentially lost as it may not be admissible in court.

Due to the nature of social media, there is a significant risk of collateral damage in the form of other, innocent parties' information being inadvertently captured alongside that of the suspected offender's. When capturing evidence from a social media profile, steps should be taken to minimise this collateral damage either before capturing the evidence, or subsequently through redaction. This might be particularly prevalent on social media profiles promoting certain events, where users are encouraged to interact with each other by posting messages or on photographs where other users may be making comments.

ACTIVITIES BY MEMBERS OF THE PUBLIC

If during the course of a complaint or enquiry, it is necessary to obtain internet material for intelligence or evidence from a member of the public, they may be asked to provide printed screen shots to corroborate the information. However, any subsequent internet research should be carried out by Tameside Metropolitan Borough Council staff and not the member of the public. This will assist with managing the activity in line with legislation and guidance. It will also reduce the risks associated with these types of enquiries. Therefore, this information should be made clear to the member of the public and documented within the relevant case notes.

USE OF INFORMATION AND MATERIAL OBTAINED

The material obtained from conducting open source internet and social media research may be used as intelligence or evidence. However, it has varying levels of value due to its reliability and authenticity. The OSC have previously stated that "particular care should be taken when using data or information obtained from open or unevaluated sources such as the internet or social networks". That is because it is not conclusive as to who posted the information. A considerable amount of information on the internet, unless being capable of time lined is historical data. Therefore, corroboration should be sought. It is currently regarded as hearsay evidence and will require corroboration.

PRESERVATION OF EVIDENCE

Evidence obtained from the internet is digital evidence. All digital evidence is subject to the same rules and laws that apply to documentary evidence.

It is also necessary to demonstrate how evidence has been recovered, showing each process through which, the evidence was obtained.
Evidence should be preserved to such an extent that a third party is able to repeat the same process and arrive at the same result as that presented to a court. Therefore, it is important that evidence obtained online is preserved and presented in a manner that is able to withstand scrutiny.

Researching, recording, storing, and using open source information regarding a person or group of people must be both necessary and proportionate, and take account of the level of intrusion against any person. The activity may also require authorisation and approval by a Magistrate under the Regulation of Investigatory Powers Act (RIPA) 2000. To ensure that any resultant interference with a person's Article 8 right to respect for their private and family life is lawful, the material must be retained and processed in accordance with the principles of the General Data Protection Regulations (GDPR).

DATA RETENTION AND DESTRUCTION OF MATERIAL

Where recorded material, in any form or media, is obtained during the course of an investigation which might be relevant to that investigation, or another investigation, or to pending or future civil or criminal proceedings, then it should not be destroyed. It should be retained in accordance with the requirements of the Data Protection Act 2018, Freedom of Information Act 2000, General Data Protection Regulations (GDPR), and any other legal requirements, including those of confidentiality, and the Council's policies and procedures regarding document retention.

Personal data gathered by the Council is subject to the Data Protection Act 2018. When considering whether to retain the data, the Council should:

review the length of time it keeps personal data;
consider the purpose or purposes it holds the information for in deciding whether (and for how long) to retain it;
securely delete information that is no longer needed for this purpose or these purposes; and
update, archive or securely delete information if it goes out of date

Due to the nature of Social Media, it is important to remember that when information is produced

as a hard copy is destroyed in line with this paragraph, that all digital copies of that evidence is likewise destroyed.

WRITTEN ACTIVITY RECORDS

Written records known as audit trails must be recorded in all cases of internet research. They should detail all the processes applied when obtaining the information and evidence. These will need to be preserved as they may later be required for oversight and to assist with any complaints that may arise with regard to breaches of privacy, or necessity and proportionality issues. Therefore, they may be required to assist with testimony in a court or tribunal relating to the conduct of the examination and procedure adopted.

An internet research form is attached at Appendix C which can be used to record the information.

REVIEWING THE ACTIVITY

During the course of conducting the internet open source research, the nature of the online activity may evolve. It is important staff continually assess and review their activity to ensure it remains lawful and compliant.

POLICY RENEWAL

This Policy will be reviewed on an annual basis.

Appendix A

Internet Research Form

Ref no:	Department:	Date:
Subject of the research Name DOB or age Address		
Offence/incident or reason for the research:		
Why it is necessary to undertake these particular enquiries in this way:		
Privacy Issues: Detail any privacy issues identified to date- how you will manage any private information obtained as a result of the research, including its storage and use:		
Confirmation of where the evidence will be stored		
Data Retention		
Authorised By		

Dated

Appendix B

Social Media Authorisation for Social Care

Ref no:	Department:	Date:
Subject of the research Name DOB or age Address		
Describe the nature of the concern (state what you think might happen to the child/vulnerable adult and assess the chances of this happening. Please confirm is this information from a credible source and how credible is the threat)		
Why it is necessary to undertake these particular enquiries in this way: (if it is possible to obtain the same information from another open source, it is not likely to be necessary)		
Privacy Issues: Detail any privacy issues identified to date- how you will manage any private information obtained as a result of the research, including its storage and use:		
Confirmation of where the evidence will be stored		
Data Retention		
Signed Print Name (Social Worker)		

Dated

Authorised By

Print Name (Service Manager)

Dated

Appendix C

Internet Research Log

Internet Research Activity Log			
Date	Activity undertaken including sites visited	By whom	Outcome of research