

PHYSICAL (CONVENTIONAL) SURVEILLANCE

POLICY AND GUIDELINES

MEMBERS (UK)

THE ASSOCIATION OF BRITISH INVESTIGATORS (ABI)

**The Association of British Investigators Limited
Registered in England and Wales # 00998568.
Registered office Brentano Suite, Elstree, WD6 3SY**

Table of Contents

1.	INTRODUCTION	3
2.	EXECUTIVE SUMMARY	3
3.	PART I – POLICY	4
A.	LEGAL REQUIREMENTS	4
B.	ETHICAL STANDARDS	6
C.	JUSTIFICATION.....	6
D.	TIME AND LOCATION.....	7
E.	RECORDING.....	7
F.	REPORTING.....	7
4.	PART II – GUIDANCE	8
A.	RISK ASSESSMENT	8
B.	REVIEW	8
C.	TRAINING	8
D.	COMMUNICATION.....	9
E.	SAFETY.....	9
F.	RESPECT FOR PRIVACY	9
G.	ACCOUNTABILITY	10
H.	TIME STAMP	10
I.	IDENTIFICATION.....	10
J.	COOPERATION WITH AUTHORITIES	11
K.	RESPECT FOR HUMAN DIGNITY	11
L.	CHILDREN AND VULNERABLE ADULT DATA.....	11
M.	HEALTH AND SAFETY	11
N.	CONFIDENTIALITY	11
O.	CONTINUOUS ASSESSMENT.....	11
P.	SUPERVISION.....	12
Q.	COMPLAINTS	12
R.	DEBRIEF AND DATA SHARING	12
S.	MONITORING AND REVIEW.....	13
5.	CONCLUSION	13

1. INTRODUCTION

- a. Physical or traditional surveillance is a crucial method for professional investigators to collect evidence across various cases. Nonetheless, it is essential that surveillance is conducted legally and adheres to ethical standards.
- b. This policy and guidance aim to offer professional investigators in the UK clear direction and best practices regarding the use of physical surveillance in their professional activities.
- c. Although it is not the ABI's policy to promote the use of GPS Electronic Devices (commonly referred to as "Trackers"), if a professional investigator decides that deploying such a device is necessary and lawful, this policy and guidance should be consulted alongside the ABI's Policy and Good Practice Guide on the Use and Deployment of Global Positioning System (GPS) Electronic Devices. This guide is available for download on the ABI website.



GPS Electronic Device Policy

2. EXECUTIVE SUMMARY

- a. The ABI expects professional investigators to conduct physical surveillance in a lawful, ethical, and professional manner.
- b. The ABI acknowledges that physical surveillance is a valuable tool for professional investigators. However, it is imperative that such activities are conducted in accordance with legal requirements and adhere to the ABI's ethical standards.
- c. For ABI members a breach of the policy outlined in Part I could lead to disciplinary action by the ABI. Furthermore, not following the guidance in Part II may be considered poor practice during any appraisal or evaluation of a professional investigator's surveillance activities.

3. PART I – POLICY

a. LEGAL REQUIREMENTS

- i. The ABI recognises that all professional investigators must comply with relevant legislation, including the Data Protection Act 2018, the UK General Data Protection Regulation (UK GDPR), The Human Rights Act 1998, and when necessary, the Regulation of Investigatory Powers Act 2000, and the Regulation of Investigatory Powers (Scotland) Act 2000 paying attention to directed and intrusive surveillance and Criminal Procedure Investigation Act CPIA 1998 (Disclosure), which is a continuing process and all relevant material is required to be retained, reviewed and disclosed until the investigation is complete.
- ii. Professional investigators can become targets for criminals or individuals with malicious intentions who masquerade as legitimate clients. It is essential to verify that an investigation does not have a concealed illegal agenda.

Example: The National Security Act 2023 identifies a specific risk where unsuspecting investigators might accept assignments linked to espionage, sabotage, or activities on behalf of foreign powers.



The most common activities agencies might be asked to assist with include:

- Surveillance, both physical and technical
- Profiling
- Tracking and locating individuals

This threat is substantially reduced if not eliminated by professional investigators being assessed as Code Members under the ABI UK GDPR Code of Conduct for Investigative & Litigation Support Services scheme.

- iii. On being presented with a case scenario, the professional investigator must first determine their role under the UK GDPR, which may be controller, joint controller, processor or sub-processor. This role will be the start position, but as the investigation develops, dictated by the activity, the role could change for some data processing.

- iv. The determination of the investigator's role is very important as the responsibilities differ. However, even as processor, the professional investigator, who may be more familiar with the UK GDPR, especially if they are a Code member to the ABI UK GDPR Code of Conduct for Investigative & Litigation Support Services scheme (approved by the Information Commissioner's Office), may as a matter of good practice, assist the controller with the controller's responsibilities.



ABI UK GDPR Code of Conduct for Investigative & Litigation Support Services

For example; the professional investigator as processor may carry out a risk assessment when they consider the investigation will involve a high risk of harm to the rights and freedoms of a data subject (an optional template data protection impact assessment can be found in the Appendices to the Code of Conduct). The processor may also assist with determining the lawful basis for the processing involved to address the client's purpose, and if that lawful basis is a legitimate interest, the processor may assist the controller in recording the legitimate interest 3-part assessment.

- v. A stated, professional investigators must identify whether their role under the UK GDPR is as a controller or a processor and communicate this role to their client to clearly establish and address their respective responsibilities. When acting as a controller, the professional investigator must fulfil the responsibilities required by data protection law, with particular emphasis on the following:
- There exists a lawful basis for the processing of any personal data involved in the assignment.
 - If the data subject's consent is the lawful basis, that it was freely given, specific, informed, and unambiguous.
 - If legitimate interest is the lawful basis, that it has met a documented legitimate interest 3-part assessment.
 - That the professional investigator has conducted and documented a data protection impact assessment for the type of case, when necessary.

- Any subcontractor instructed by the professional investigator as processor is contracted in writing including the Article 28(3) terms.
 - The assignment will be conducted within the data protection principles.
- vi. The professional investigator has provided the client with a written proposal, which on acceptance could form the contract. The proposal to include:
- An outline of the case scenario.
 - A clearly defined purpose and lawful basis for the assignment.
 - The objectives.
 - Methodology.
 - Controller's permission to outsource any data processing activity.
 - The professional investigator's UK GDPR role and any special compliance matters.
 - The fee structure and payment terms.
 - Time frame and when the client may expect a report.

b. ETHICAL STANDARDS

- i. The ABI mandates that its affiliated professional investigators uphold the highest ethical standards, including respect for individuals' privacy and dignity.
- ii. Professional investigators are expected to consistently act with integrity and honesty, avoiding any behaviour that could be perceived as harassment or intimidation.

c. JUSTIFICATION

- i. Physical surveillance must only be conducted when it is necessary and proportionate to the case.
- ii. Professional investigators are required to have a lawful basis for conducting surveillance. When it is based on legitimate interest, they must ensure that this interest aligns with the reasonable expectations of the individual and outweighs any potential harm or intrusion into their privacy.

d. TIME AND LOCATION

- i. Professional investigators must confine the duration and location of surveillance activity to ensure it is both necessary and proportionate to the case.
- ii. The professional investigator must refrain from conducting surveillance in locations where the individual has a reasonable expectation of privacy, such as inside their home. Care and justification are required for sensitive locations, including places of worship, medical consultation venues, and similar places.

e. RECORDING

- i. Professional investigators must:
 - Ensure that all surveillance recordings are conducted legally and in compliance with ethical standards. This includes employing the least intrusive methods and mechanisms of recording appropriate for the situation, such as determining whether the recording should be limited to audio, video, or still images.
 - Not record conversations where individuals have a reasonable expectation of privacy, such as confidential discussions with their legal representatives.
 - Ensure that recordings are stored securely and are destroyed once they are no longer needed.

f. REPORTING

- i. Professional investigators must provide accurate reports of surveillance activities.
- ii. Reports must be clear, concise, and objective. They must include all relevant details such as the date, time, location, and duration of the surveillance.

4. PART II – GUIDANCE

a. RISK ASSESSMENT

- i. As a matter of good practice, professional investigators should compile an Operational Order for a surveillance using the following framework and titles.
 - a. IIMACRH Operational Order to be destroyed in compliance with the UK GDPR guidelines on destruction when no longer required.
 - b. Information
 - c. Intention
 - d. Administrative
 - e. Communication
 - f. Risk Assessment
- ii. During the risk assessment, the professional investigator should evaluate if the subject under surveillance is of interest to law enforcement agencies such as the police, DWP, HMRC, or Trading Standards. This could increase the risk and potentially affect any ongoing investigations.

b. REVIEW

- i. Professional investigators should periodically evaluate the use of physical surveillance in their investigations to confirm that it remains necessary and proportionate, and they should document this evaluation.
- ii. Additionally, professional investigators should ensure that surveillance activities are consistently reviewed by a senior member of their organisation.

c. TRAINING

- i. Professional investigators who lack extensive experience or qualifications, such as those gained through prior military or police service, should contemplate enrolling in an appropriate course to obtain an accredited qualification. Regardless, professional investigators must ensure that all their operatives have undergone suitable training and are informed of the legal and ethical standards relevant to their work.

- ii. Professional investigators should routinely offer training to their operatives to ensure they remain informed about any updates in legislation or industry best practices.
- iii. Comprehensive debriefs should be conducted after each surveillance activity to identify mistakes, address misunderstandings, and highlight areas for improvement.

d. COMMUNICATION

- i. Professional investigators must communicate clearly with their clients regarding the use of physical surveillance and its limitations to effectively manage client expectations.
- ii. They should encourage clients to seek legal advice before proceeding with surveillance and must ensure they have received clear written instructions from the client before conducting any surveillance.

e. SAFETY

- i. Professional investigators must ensure that all surveillance activities are carried out safely.
- ii. They should avoid any actions that could jeopardise their own safety or that of others and must steer clear of behaviour that could be perceived as threatening or intimidating.

f. RESPECT FOR PRIVACY

- i. Professional investigators must always respect the privacy and dignity of individuals.
- ii. They should avoid conducting surveillance that may be deemed intrusive or excessive and must maintain the highest standards of professionalism and discretion in their work.

g. ACCOUNTABILITY

- i. Professional investigators must be accountable for their actions and should be ready to justify their use of physical surveillance to their clients, the public, and any regulatory entities.
- ii. They are required to maintain accurate records of all surveillance activities and be prepared to present those records to relevant authorities if requested.
- iii. Each professional investigator holds vicarious liability concerning accountability and disciplinary issues for the actions of any operatives they employ.

h. TIME STAMP

- i. Wherever possible, all footage should include a visible timestamp with the date. If this isn't feasible, the footage should be authenticated by referencing it in the surveillance log. This can be done with a contemporaneous log entry or an addendum made during the debrief.
- ii. When capturing video or still images, professional investigators and their operatives must be aware of any incidental intrusion that may appear in the footage or other image files. They should evaluate whether there is a need to pixelate, obscure, or otherwise edit this data.

i. IDENTIFICATION

- i. Professional investigators must always carry identification and be ready to present it to anyone with a legitimate reason to request it, as long as doing so does not compromise the operation. This practice helps prevent misunderstandings and ensures the member is not mistaken for someone else.
- ii. The professional investigator should have a pre-prepared cover story and appropriate props or identity card to use if approached by a third party. If an operation is at risk of being compromised, observations should be immediately concluded, and the client should be informed as soon as possible.

j. COOPERATION WITH AUTHORITIES

- i. Professional investigators are expected to cooperate with the police and other authorities when requested.
- ii. However, while cooperating, professional investigators must also consider their responsibilities under data protection laws and their duty of confidentiality. This includes sharing information about their surveillance activities only in compliance with legal requirements and any directives from the authorities.

k. RESPECT FOR HUMAN DIGNITY

Professional investigators should uphold the dignity of individuals under surveillance and refrain from engaging in behaviour that could be considered demeaning or humiliating.

l. CHILDREN AND VULNERABLE ADULT DATA

Professional investigators should refrain from using surveillance tactics on children or vulnerable adults unless it is necessary and proportionate to the situation.

m. HEALTH AND SAFETY

Professional investigators should implement appropriate health and safety measures while conducting surveillance, especially in hazardous or challenging environments, to ensure the safety of all involved.

n. CONFIDENTIALITY

Professional investigators must preserve the confidentiality of information obtained during surveillance and ensure it is never disclosed to any unauthorised individuals.

o. CONTINUOUS ASSESSMENT

- i. Professional investigators should continuously assess the necessity and proportionality of their surveillance activities. Surveillance must be discontinued when it is deemed unnecessary or disproportionate.

- ii. Every effort should be made to avoid capturing third parties in footage. If unavoidable, professional investigators should consider pixelating, obscuring, or editing any video or still images to protect third-party identities on all working copies, thereby minimising collateral intrusion.

p. SUPERVISION

- i. Professional investigators must ensure that their operatives receive appropriate supervision to conduct physical surveillance lawfully and ethically. This includes providing training on the ABI code of ethics and professional standards, as well as the guidance outlined in this document.
- ii. They should also provide ongoing supervision and support to their operatives to ensure that they adhere to good practice and maintain ethical standards in their conduct.

q. COMPLAINTS

- i. Professional investigators must have an internal complaints and monitoring system in place to ensure that any complaints or concerns are addressed promptly and appropriately. This system should include a mechanism for individuals to file complaints regarding their conduct and/or their operatives.
- ii. The internal complaints system of an ABI member does not alter the ABI discipline process outlined in the ABI bylaws.

r. DEBRIEF AND DATA SHARING

- i. Professional investigators should conduct a thorough debrief with all operatives involved as soon as practical following surveillance. This debrief should focus on discussing findings and addressing any issues of concern that arose during the operation while they are still fresh in the operatives' minds.
- ii. All footage and reports that are shared should be protected with a password to ensure security and confidentiality.

s. **MONITORING AND REVIEW**

- i. The ABI will oversee the use of physical surveillance activities conducted by its members and will routinely review this policy and guidance. This is to ensure that it remains relevant and effective over time.
- ii. Professional investigators are encouraged to provide feedback to the ABI regarding any issues or concerns related to the current policy or guidance. They should also be prepared to implement any necessary changes that may arise from such feedback or from regular policy reviews.

5. CONCLUSION

- a. The ABI acknowledges that physical surveillance is a valuable tool for professional investigators. However, it is imperative that such activities are conducted in accordance with legal requirements and adhere to the ABI's ethical standards.
 - b. For ABI members a breach of the policy outlined in Part I could lead to disciplinary action by the ABI. Furthermore, not following the guidance in Part II may be considered poor practice during any appraisal or evaluation of a professional investigator's surveillance activities.
-