




National Protective
Security Authority

Guidance **Social Media Auditors**

December 2023



Contents

Introduction		3
Auditor or Hostile Reconnaissance?		4
Engagement		5
Offences		10
Drone Usage		11
Police – When to Call?		12
Further Reading		13



Introduction

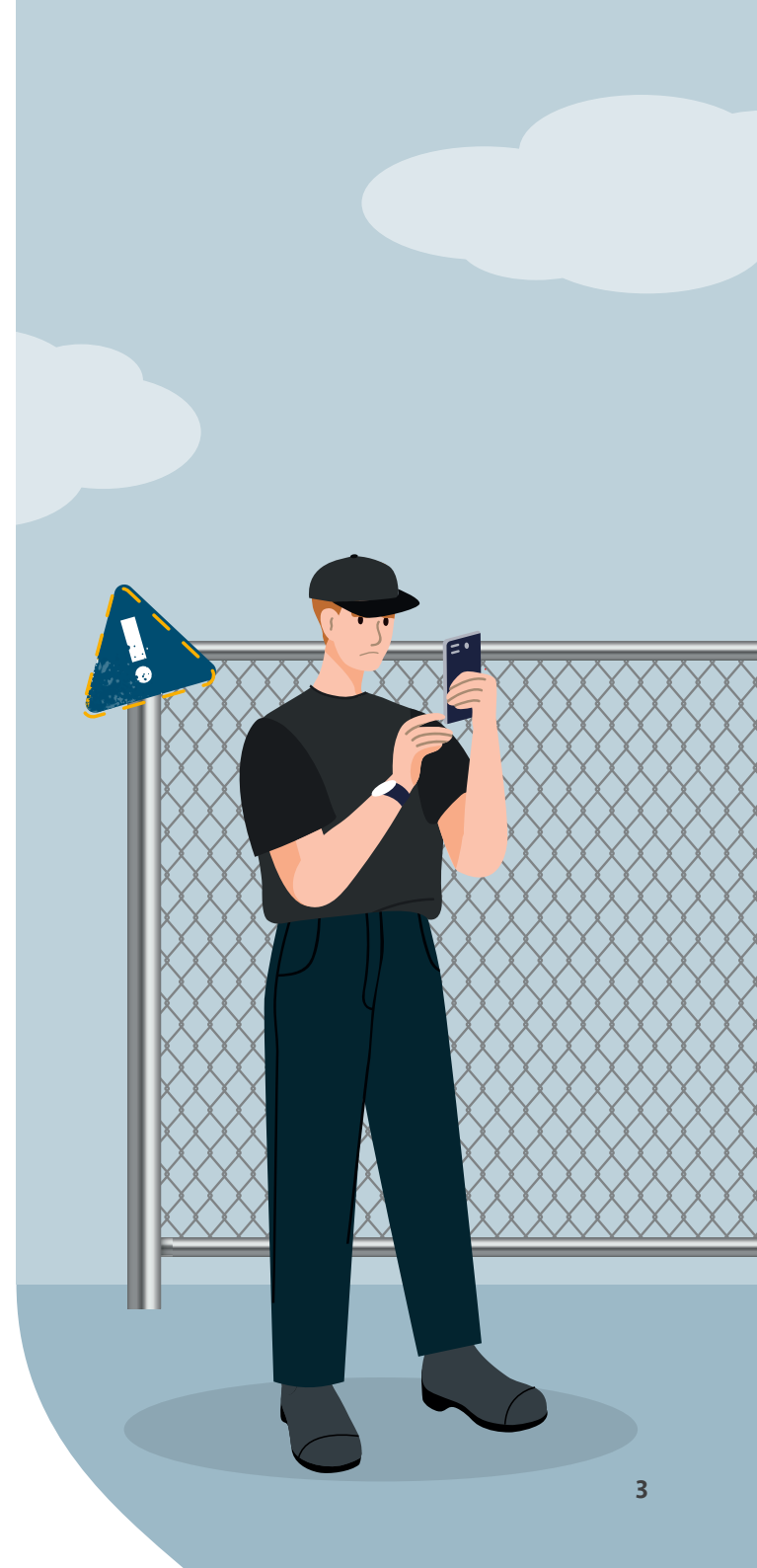
There is a small but increasing number of reports within the United Kingdom involving individuals who attend premises and outside spaces, with the aim of capturing staff and property on camera, the content from which is often uploaded to social media and video platforms. We refer to them as Auditors in this guidance as it's the term most associated with them online. Other terms include social media auditors and citizen journalists.

Auditors take advantage of the understandable concerns from personnel when staff and premises are photographed or filmed. Auditors often attempt to provoke staff and security in order to elicit heightened reactions, at times asserting that staff are overstepping legal boundaries. They are well versed in their own rights and frequently cite legislation when challenged.

It is not an offence to be an Auditor or to film personnel and property from a place the Auditor is allowed to be. This includes filming private property with a drone where a drone is allowed to fly.

Auditing activity is mostly harmless, and the amount of compromising information gathered by filming vehicles, personnel, equipment or the facility itself is generally minimal. Issues typically arise when staff and security engage in a hostile manner, by quoting legislation incorrectly, or by giving inaccurate statements such as "You are not allowed to film here".

While the Auditors themselves might not have hostile intent, the content they create and post online could be viewed by genuine hostile actors. As such, conveying an air of a professional security culture is helpful – such as highlighting the CCTV which alerted you to their presence – but without giving unnecessary insight into your security infrastructure or procedures.



Auditor or Hostile Reconnaissance?

Whilst filming sensitive locations may be an indication of a hostile intent, hostile reconnaissance is almost always done covertly. Auditors want to be noticed to create engagement opportunities: they conduct their filming openly, often narrating their footage.

Individuals conducting such activities should be engaged politely to confirm their intent, in a manner that makes it clear that the Auditor is being observed but without being confrontational. Staff should be aware of the behaviours that may indicate Hostile Reconnaissance¹.



Note 1: Refer to See, Check and Notify (SCaN) guidance on Hostile Reconnaissance.

npsa.gov.uk/see-check-and-notify-scan

Engagement

Everyone has a role to play in security. There have been incidents when unsuspecting members of staff have been approached when entering or exiting their workplaces.

Because Auditors can rely on confusion and intimidation, making staff aware – and prepared – is an important aspect of protecting against such tactics.

It is important that all staff remain polite and professional if responding to a situation where someone is recording premises and/or staff. When engaging, remember that your first words will often dictate the tone of the interaction.

When interacting with suspected Auditors, we recommend a **CALM approach** – Chat, Assess, Limit, Monitor.

If you're familiar with the See, Check and Notify (SCaN) guidance, this would align as part of the 'Check' section.



CALM

Chat

First, engage suspected Auditors in a friendly manner. A professional greeting will often work better than a more confrontational approach:

- "How's it going today?"
- "I was curious what you were doing out here"
- "Our control room noticed you around the area and have asked me to see what you are doing, and if you need any help?"

Remember that the goal of Auditing is often to generate controversial content. A friendly opening will minimise the risk of this happening while ensuring you remain vigilant and a maintain a strong security culture.

How's it going today?
I was curious what you were doing out here.

I uh...

Warning

Do not enter
without pass


CALM

Assess

Next, confirm the suspected Auditor's intent while continuing to evaluate for other potential threats they might pose, or may provide a distraction for.

Auditors will often either identify themselves as a social media Auditor, or state that they do not need to provide a reason to film. If the Auditor provides a name of social media account, this could be noted down to check at a later point.

If you feel the Auditor's behaviour may represent a genuine security risk or feel there is a risk for the personal information of staff to be misused, call the police. The police will assess whether they need to attend based on the information provided. The incident record will also assist in building an intelligence picture around such activity.



If you feel the Auditor's behaviour may represent a genuine security risk or feel there is a risk for the personal information of staff to be misused, call the police.

CALM

Limit

Thirdly, aim to keep interactions with Auditors as short as you can while maintaining your security presence.

Auditor activities rely on generating and maintaining negative encounters, so by limiting interactions you minimise the scope for negative content from video or audio recordings.

Everyone interacting with Auditors should be particularly mindful of avoiding the use of inappropriate or offensive language.

Remember: the goal for Auditors is often to provoke such reactions in order to generate online engagement.



CALM

Monitor

Lastly, you should continue to monitor Auditors to ensure that they don't escalate into a threat, such as attempting to breach a perimeter.

Such monitoring can be done from a distance to avoid unnecessary encounters, if you are able to do so effectively.

If escalation does occur, or you have other concerns, you should notify the police.



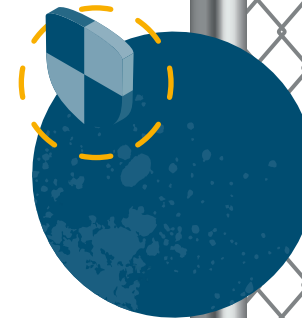
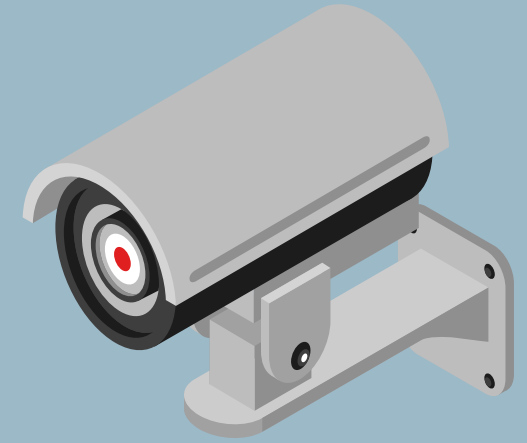
Offences

There are no powers prohibiting the taking of photographs or video in a public place. Therefore, members of the public should not be prevented from doing so.

There can be uncertainty around what areas of a property are privately and publicly owned. Site security should be clear where the borders of their property and land begin, including ensuring there is adequate signage and perimeter fencing.

There have been occasions where Auditors have gained access to private property. Existing security plans should be used in these instances, which should include contacting the police if there are any concerns for safety or possible criminal activity.

While the Auditors themselves might not have hostile intent, the content they create and post online could be viewed by genuine hostile actors. As such, conveying an air of a professional security culture is helpful – such as highlighting the 24-hour live monitored CCTV which alerted you to their presence – but without giving unnecessary insight into your security infrastructure or procedures.



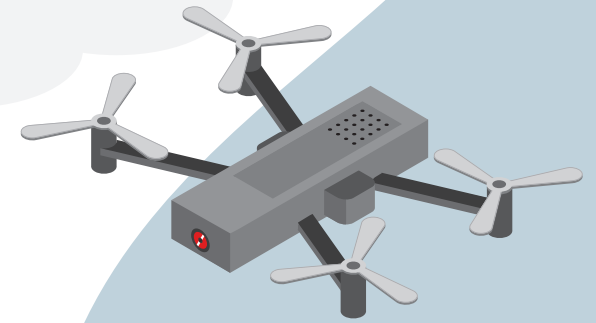
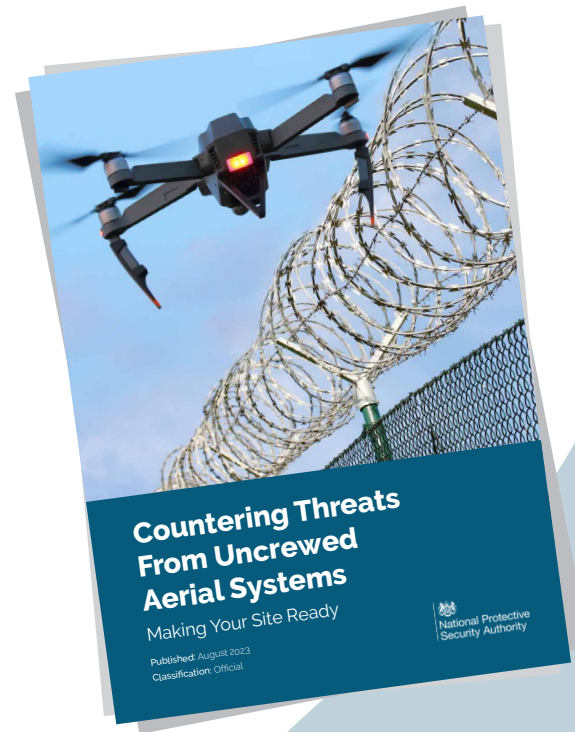
Drone Usage

Drones are largely allowed to fly in UK airspace without requiring permission. There are a few exceptions, including:

- Flight Restriction Zones (FRZs) – usually around airports and aerodromes
- Airspace Restriction Order (ARO) areas – usually around sensitive or protected sites. AROs can be permanent or temporary
- Over crowded places, regardless of drone size

There are no laws prohibiting the taking of images or video from a public place – and that can include the airspace over or near buildings. Invasion of Privacy is not a criminal offence and is rarely a police matter.

This does not mean Auditors cannot commit offences when flying a drone over or near buildings. The police should be called if you believe an offence is being committed.



Note 2: Refer to NPSA Counter Uncrewed Aerial Systems (C-UAS) Guidance
npsa.gov.uk/counter-uncrewed-aerial-systems-c-uas

Police – When to Call?

Call 101:

If after an encounter you still have concerns, contact the police who can offer advice.

Call 999:

If there are any concerns that there is an immediate risk, or a crime may be committed, call the police providing as much information as possible.

Note: Trespassing is not classed as a criminal offence, but police may attend to assess if there are any offences or provide advice.



Further Reading:

NPSA: Protecting Your Assets: Deter, Detect, Delay, Mitigate and Response
<https://www.npsa.gov.uk/protecting-your-assets>

NPSA: Scan Check and Notify (SCaN) guidance on Hostile Reconnaissance.
<https://www.npsa.gov.uk/see-check-and-notify-scan>

NPSA: Counter Uncrewed Aerial Systems (C-UAS) Guidance
<https://www.npsa.gov.uk/counter-uncrewed-aerial-systems-c-uas>





Disclaimer

This document has been prepared by the National Protective Security Authority (NPSA). This document is provided on an information basis only, and whilst NPSA has used all reasonable care in producing it, NPSA provides no warranty as to its accuracy or completeness. To the fullest extent permitted by law, NPSA accepts no liability whatsoever for any expense, liability, loss, damage, claim, or proceedings incurred or arising as a result of any error or omission in the document or arising from any person acting, refraining from acting, relying upon or otherwise using the document. You should make your own judgment with regard to the use of this document and seek independent professional advice on your particular circumstances.

© Crown Copyright 2023

