SAFETY HUB PRACTICAL TOOL

When Staff Are Filmed or Recorded: An Employer's Action Guide

Practical guidance and adaptable workplace procedures for managing recordings, protecting employees and responding to harmful material shared online.

About this resource

Employees working in housing, local authorities, healthcare, social care, charities, enforcement and other public-facing services may be filmed, photographed, recorded or livestreamed while carrying out their duties.

Recording technology is now commonplace. Employees may encounter mobile phones, doorbell cameras, domestic CCTV, smart watches, smart glasses, baby monitors, pet cameras, smart speakers and other connected devices.

Some recordings are made openly. Others may be captured without employees realising that recording is taking place.

Recordings can be made for legitimate reasons, including keeping a record of a conversation or supporting a complaint. However, recordings may also be used to intimidate employees, expose their personal information, misrepresent an incident or encourage online harassment.

This guide explains how employers can protect staff, respond proportionately and establish practical procedures for managing these situations.

It includes an adaptable workplace policy that organisations can review and adopt.

> Important: Recording someone without their consent is not automatically unlawful. The legal position depends on the circumstances, the nature of the recording, how it is used and the applicable law.

Organisations should obtain appropriate legal and information governance advice before adopting restrictions or taking formal action.

Part One: Understanding the Risks

1 How employees may be recorded

Recording can take place in many everyday working situations.

Examples include:

- A housing officer being filmed during a home visit.
- A receptionist being recorded during a difficult conversation.
- An enforcement officer being filmed while issuing a penalty notice.
- A support worker being recorded by an indoor security camera.
- A telephone conversation being recorded without prior notice.
- A visitor livestreaming an encounter to social media.
- A smart doorbell capturing an employee approaching or leaving a property.

- Smart glasses recording video without an obvious handheld device.
- A smart watch or mobile telephone recording audio.
- A mobile phone being left in a room with a recording application running.
- A baby monitor or pet camera transmitting audio and video remotely.
- A smart speaker or connected device being used to capture or transmit conversations, where its actual capabilities permit this.

Employees should not assume that every device is recording continuously or that all devices have the same capabilities.

The concern is not simply the presence of equipment. It is whether recording, monitoring or subsequent publication creates a risk to confidentiality, privacy, safeguarding or personal safety.

2 Legitimate recording and unacceptable behaviour

People may have legitimate reasons to record interactions with organisations.

For example, someone may wish to:

- Keep an accurate record of what was said.
- Support a complaint.
- Document the conduct of a public-facing employee.
- Obtain evidence of an incident.
- Help them recall information discussed during an appointment.

An organisation should not automatically describe these activities as harassment or unlawful conduct.

However, concerns may arise where someone:

- Uses recording equipment to intimidate an employee.
- Follows or threatens a member of staff.
- Records confidential information about another person.
- Publishes an employee's private information to encourage harassment.
- Shares footage alongside threats or abusive allegations.
- Repeatedly targets an identifiable employee.
- Uses edited or fabricated footage to encourage hostility or intimidation.

Employers should assess the behaviour, context and risks rather than assuming that recording itself proves wrongdoing.

3 What employees should do when recording is noticed

Employees should remain professional and avoid confrontation.

Where appropriate, they can:

- Acknowledge that recording is taking place.
- Explain the purpose of the visit or conversation.
- Clarify any relevant confidentiality restrictions.
- Ask for sensitive conversations to take place in a more suitable setting.
- Seek managerial assistance if the situation becomes difficult.
- Withdraw where a genuine safety concern develops.

An appropriate response might be:

> *"I understand that you are recording our conversation. I am happy to explain the organisation's position, but I cannot discuss another person's confidential information."*

Where the situation becomes threatening:

> *"I am concerned about how this conversation is developing. I am going to end the visit now and ask my manager to contact you about the next steps."*

Employees should not seize equipment, demand access to recordings, attempt to delete footage or physically obstruct a camera.

They should follow their organisation's procedures and report significant concerns.

4 Recording equipment in homes and other premises

Employees undertaking home visits should recognise that recording equipment may already be installed.

This may include:

- Video doorbells.
- Indoor CCTV.
- Baby monitors.
- Pet cameras.
- Smart speakers.
- Smart glasses.
- Mobile phones and tablets.
- Audio-recording devices.
- Other connected monitoring equipment.

Some devices allow remote viewing, live audio monitoring, motion-triggered recording or access to recordings stored in the cloud.

Employees should avoid making assumptions about a device's capabilities.

If a device raises a concern about confidentiality, safeguarding or personal safety, the employee should explain the concern and seek a suitable alternative.

Employees should not search a property for hidden equipment or attempt to disable devices.

Where covert recording is suspected, report the concern to a manager for assessment.

Part Two: When Recordings Are Shared Online

5 Recognising harmful online publication

A video, photograph or audio recording may be uploaded to Facebook, TikTok, Instagram, YouTube or another platform.

Some posts may be legitimate criticism or evidence supporting a complaint.

Others may create risks by:

- Identifying an employee and encouraging people to confront them.
- Publishing their home address or personal contact details.
- Naming family members or revealing their whereabouts.
- Making threats of violence.
- Encouraging repeated unwanted contact.
- Sharing discriminatory or sexually abusive material.
- Misrepresenting an incident through selective editing.
- Using artificial intelligence to fabricate images, speech or video.
- Impersonating an employee or creating a false account in their name.

The organisation should distinguish criticism from threats, harassment, stalking, intimidation and other potentially unlawful conduct.

Not every offensive or misleading publication is automatically a criminal offence.

6 Immediate action when harmful material is discovered

The employee affected should not be expected to deal directly with the uploader.

Employees should:

- Inform their manager promptly.
- Avoid replying to comments or messages.
- Avoid confronting or privately contacting the uploader.
- Avoid publishing their own rebuttal.
- Avoid encouraging colleagues or friends to challenge the person online.
- Avoid unnecessarily sharing the material with others.

Managers should take responsibility for assessing the incident and coordinating the response.

Where there is an immediate threat to life or safety, contact emergency services.

In the United Kingdom, call 999 in an emergency.

In the Republic of Ireland, call 999 or 112.

7 Preserve the evidence

Evidence should be captured promptly, where safe and lawful, because online content can be edited or removed.

An authorised manager or designated employee should consider preserving:

- The direct link to the post.
- The platform name.
- The uploader's account name and profile link.
- The date and time the material was discovered.
- Screenshots of the post and its accompanying text.
- Relevant comments, including threats.
- Screenshots showing disclosure of private information.
- The video, audio or image file, where lawful and technically possible.
- Relevant messages or correspondence.
- Evidence of repeated publication or contact.
- The names of employees or witnesses who discovered the material.

Where possible, preserve original files and available metadata.

Do not alter the original evidence. If cropped images or extracts are required for reporting, retain the original separately.

Keep an evidence record showing who collected the material, when it was collected and where it is securely stored.

Access should be limited to authorised personnel.

> Important: If material may contain child sexual abuse imagery, intimate images shared without consent or other illegal content, do not routinely download, copy or forward it. Seek urgent police or specialist advice about safe evidence preservation.

Do not delay urgent police reporting while attempting to collect evidence.

8 Assess the risk and decide whether to contact the police

Managers should consider:

- Does the material contain a credible threat?
- Has the employee's home address or other private information been disclosed?
- Is the employee being repeatedly targeted?
- Are other people being encouraged to identify, contact or confront the employee?
- Does the publication involve suspected stalking or harassment?
- Are there safeguarding concerns?
- Is the employee or their family at risk?
- Has confidential organisational information been disclosed?
- Does the material appear manipulated or fabricated?
- Is there a wider risk to other employees?

Suspected criminal conduct should be reported to the police where appropriate.

In the United Kingdom, use 999 for an emergency and 101 or the relevant police reporting service for non-emergency matters.

In the Republic of Ireland, contact An Garda Síochána through the appropriate reporting arrangements.

Record police reference numbers, advice received and decisions made.

9 Request removal from the social media platform

An authorised manager should report harmful material using the platform's reporting arrangements.

Depending on the circumstances, relevant reporting categories may include:

- Threats or violence.
- Harassment or bullying.
- Stalking or intimidation.
- Sharing private information.
- Impersonation.
- Manipulated or misleading content.

Provide accurate information and relevant evidence.

Keep a record of:

- The date of the report.
- The platform contacted.
- The content reported.
- The reason for requesting removal.
- The report reference number.
- Any response received.
- Whether an appeal or further review is required.

A platform may decline to remove material that does not breach its rules or applicable law.

An organisation should not assume that every disputed recording can be removed.

10 Contacting the person responsible for uploading the material

Where the uploader is known, an organisation may consider sending a formal written request for removal.

This should be undertaken by an authorised manager or legal representative, not by the employee affected.

Before making contact, consider:

- Whether contact could escalate the situation.
- Whether the police are investigating.
- Whether the person has previously threatened employees.
- Whether the organisation has a sound basis for requesting removal.
- Whether the material forms part of a legitimate complaint.
- Whether specialist legal advice is required.

A suitable example is:

> *"We are aware of material published on [platform] on [date] involving a member of our staff. We are concerned that the accompanying information may expose the employee to threats, harassment or unwanted contact. We request that you remove the identified material and refrain from publishing personal information or encouraging others to target the employee. If you wish to raise a complaint about the original incident, our formal complaints procedure remains available."*

Adapt the wording to the circumstances.

Do not threaten automatic eviction, arrest or prosecution.

Do not claim that recording without consent is always unlawful.

Do not contact the uploader if doing so could compromise a police investigation, increase danger or escalate suspected stalking or harassment.

Retain a copy of all correspondence.

11 Supporting the employee

Online targeting can have a significant impact on employees, particularly where personal details or family members are involved.

Managers should consider:

- Immediate welfare and reassurance.
- Whether the employee feels safe at work.
- Temporary changes to home visits or lone working.
- Additional security arrangements.
- Support through occupational health or an employee assistance programme.
- Assistance reviewing personal information exposed online.
- Appropriate safeguarding measures.
- Whether colleagues need to be informed about a credible threat.
- Follow-up contact and ongoing monitoring.

The employee should not be blamed for being targeted.

Any changes to duties or working arrangements should be discussed sensitively and reviewed.

12 AI-generated and manipulated recordings

Artificial intelligence can be used to alter photographs, generate convincing speech, change facial expressions or produce fabricated video.

Selective editing and misleading captions can also change how an incident appears to viewers.

Where manipulation is suspected:

- Preserve the original published material.
- Record exactly what appears inaccurate.
- Seek the original recording or other relevant evidence where available.
- Avoid publicly repeating unsupported allegations.
- Consider whether specialist technical assessment is needed.
- Report threats, impersonation or harmful manipulation through the appropriate channels.

Do not state that material is AI-generated unless there is a reasonable evidential basis for that conclusion.

Part Three: Preventing Problems and Protecting Employees

13 Reducing unnecessary exposure of employee information

Organisations should review how much personal information they routinely make available about public-facing employees.

This includes:

- Full names on staff identification badges.
- Direct email addresses containing full names.
- Personal contact details.
- Staff photographs and profiles on public websites.
- Names included in correspondence.
- Public staff directories.
- Details of working locations or shift patterns.

For higher-risk roles, consider whether a first name and a dedicated public-facing staff identifier would provide sufficient accountability without unnecessarily exposing an employee's surname.

For example:

Sarah | Housing Officer | Staff ID: H0472

The identifier should be a dedicated public-facing reference, not a payroll number or another confidential personnel identifier.

This is a risk-based option, not a universal legal requirement. Some roles have statutory, professional or operational identification requirements.

Employers should preserve accountability and ensure complaints can be traced internally to the appropriate employee.

14 Training and employee awareness

Employees should understand:

- Their organisation's recording policy.
- The difference between legitimate recording and threatening behaviour.
- How to respond calmly when being filmed.
- When to seek assistance or withdraw.
- How smart devices may be used to record interactions.
- How to report suspected covert recording.
- Why they should not confront online uploaders.
- How evidence should be preserved.
- How to protect their digital footprint.

- What support is available after an incident.

Training should use realistic scenarios relevant to employees' duties.

Managers should understand their responsibilities for risk assessment, incident reporting, evidence preservation, police liaison, online platform reporting and employee welfare.

Part Four: Adaptable Workplace Policy

15 Model organisational policy

Policy title: Recording Employees and Responding to Online Misuse

The following wording can be adapted by an organisation before formal adoption.

Policy statement

[Organisation] recognises that employees may be filmed, photographed or recorded while carrying out their duties.

We respect legitimate recording, privacy, accessibility and complaint rights. We are equally committed to protecting employees from threats, intimidation, harassment and other foreseeable risks arising from recording or online publication.

We will assess incidents fairly and proportionately, taking account of employee safety, service-user rights, confidentiality, safeguarding and applicable law.

Scope

This policy applies to employees, agency workers and contractors acting on behalf of [Organisation], including during home visits, reception duties, enforcement activity, telephone contact, public-facing appointments and remote working interactions.

Employee responsibilities

Employees must:

- Follow organisational safety procedures.
- Remain professional when recording is noticed.
- Protect confidential information.
- Report significant recording-related concerns.
- Withdraw or seek assistance where a genuine safety risk develops.
- Avoid confronting uploaders or responding to online harassment.
- Preserve available evidence in accordance with organisational instructions.

Manager responsibilities

Managers must:

- Assess reported risks promptly.
- Protect employees and arrange appropriate support.
- Ensure evidence is preserved securely.
- Consider police reporting where appropriate.
- Coordinate platform reports and removal requests.
- Seek specialist advice where necessary.
- Maintain accurate incident records.
- Review relevant risk assessments and working arrangements.
- Ensure follow-up action is completed.

Information governance

Personal information and recorded evidence must be handled in accordance with applicable data protection law and organisational procedures.

Evidence must be stored securely, accessed only where authorised and retained in accordance with an appropriate retention schedule.

Data protection concerns, suspected breaches and requests for personal information must be referred to the appropriate organisational lead.

Complaints and service-user rights

Legitimate complaints and lawful recording must not automatically result in punitive action or withdrawal of essential services.

Any restrictions on contact or service arrangements must be justified, proportionate, lawful and subject to appropriate review.

Policy review

This policy should be reviewed following significant incidents, changes in recording technology, relevant legal developments or changes to organisational risk assessments.

16. Document control

Field	Organisation entry
Organisation	To be completed
Policy owner	To be completed
Approved by	To be completed
Approval date	To be completed
Effective date	To be completed
Review date	To be completed
Version	To be completed

17. Incident response checklist

- [ ] Confirm the employee's immediate safety.
- [ ] Assess threats to the employee and their family.
- [ ] Instruct the employee not to engage with the uploader.
- [ ] Preserve available evidence safely and lawfully.
- [ ] Record links, screenshots, account details and relevant comments.
- [ ] Consider whether police involvement is necessary.
- [ ] Report harmful material to the platform.
- [ ] Consider a formal removal request where safe and appropriate.
- [ ] Refer data protection or safeguarding concerns.
- [ ] Arrange appropriate employee welfare support.
- [ ] Review visiting, lone working and security arrangements.
- [ ] Record decisions, actions and reference numbers.
- [ ] Set a follow-up date and confirm outstanding actions.

18. Further guidance

For additional information, consult relevant official guidance from:

- The Information Commissioner's Office, for UK data protection and video surveillance: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/
- The Data Protection Commission, for organisations operating in the Republic of Ireland: https://www.dataprotection.ie/
- Police.uk: https://www.police.uk/
- Police Scotland: https://www.scotland.police.uk/
- An Garda Síochána: https://www.garda.ie/
- Ofcom, for online safety and reporting arrangements: https://www.ofcom.org.uk/
- The Health and Safety Executive or the relevant national workplace safety authority: https://www.hse.gov.uk/violence/

Useful Safety Hub resources:

- When Staff Are Recorded or Livestreamed: https://www.safetysolutionstraining.co.uk/knowledge/modern-recording-risks
- Protecting Staff from Online Targeting and Harassment: https://www.safetysolutionstraining.co.uk/knowledge/workplace-digital-safety-online-harassment
- Body-Worn Cameras at Work: https://www.safetysolutionstraining.co.uk/knowledge/body-worn-cameras-at-work
- Lone Worker Safety Centre: https://www.safetysolutionstraining.co.uk/knowledge/lone-worker-safety

Important information

This resource is provided by Safety Solutions Training Ltd as general workplace safety guidance and an adaptable policy template.

It is not legal advice and does not establish that any particular recording, publication or conduct is unlawful.

Organisations must review the policy against their own activities, legal obligations, workforce, risk assessments and internal procedures before adoption.

Legal requirements differ between England, Wales, Scotland, Northern Ireland and the Republic of Ireland.

Safety Solutions Training Ltd

https://www.safetysolutionstraining.co.uk/knowledge