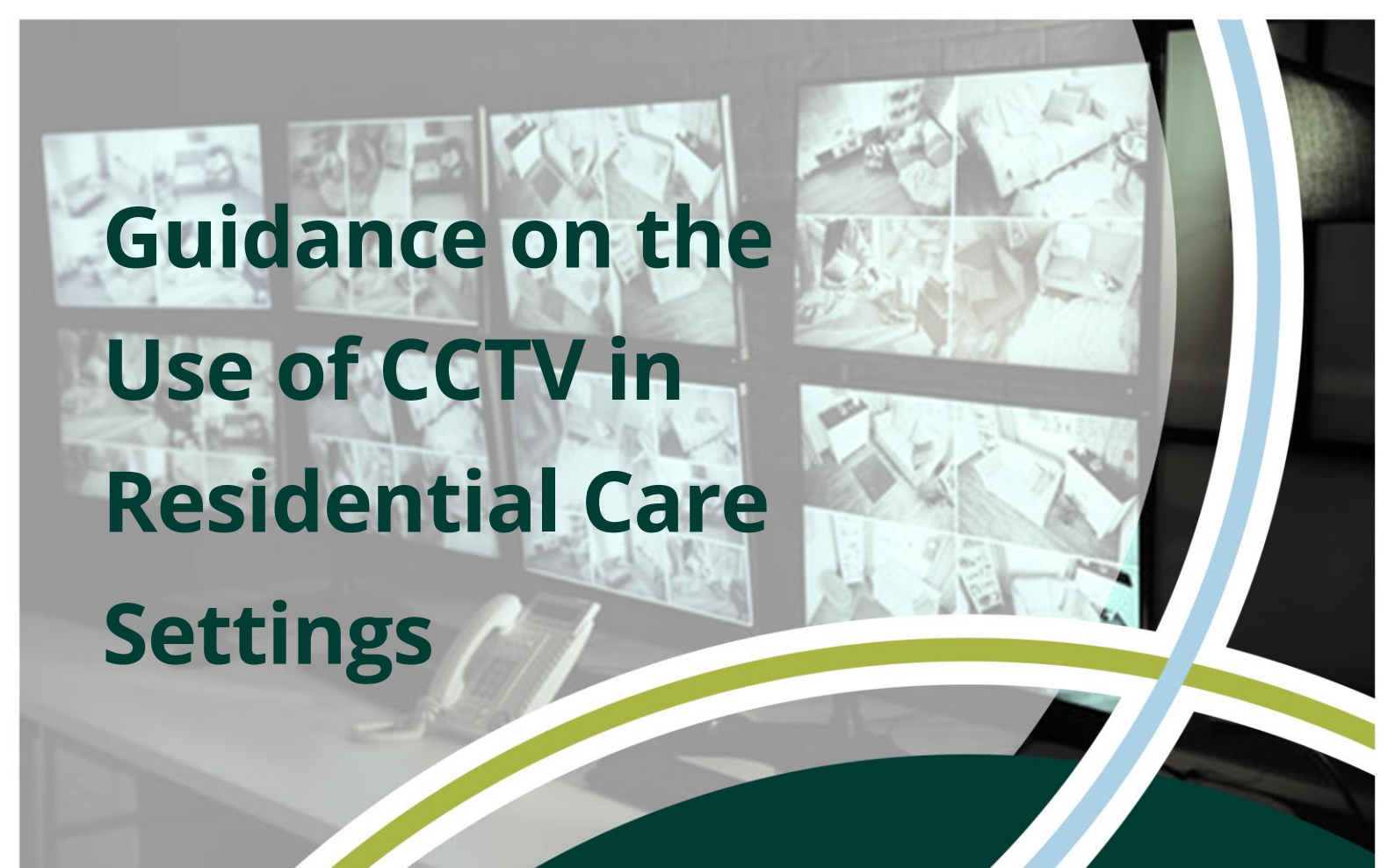




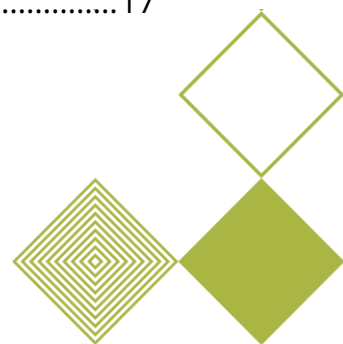
Guidance on the Use of CCTV in Residential Care Settings

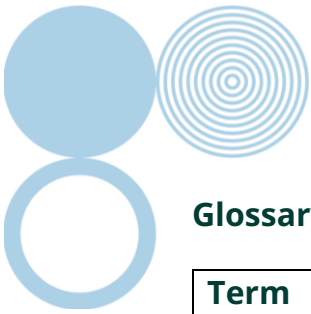
August 2026



Contents

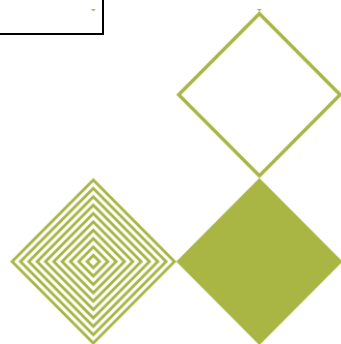
Introduction	6
Heightened expectations of privacy	7
Purpose of processing personal data using CCTV	7
Necessity and Proportionality	8
Lawful basis.....	9
Transparency	11
CCTV policy and signage	11
Live-view observation cameras.....	12
Covert video surveillance.....	13
Other monitoring technologies	13
Technical and organisational measures.....	14
Rights of individuals.....	14
Disclosure of CCTV	15
Data Protection Impact Assessments (DPIAs)	16
Ongoing review.....	17

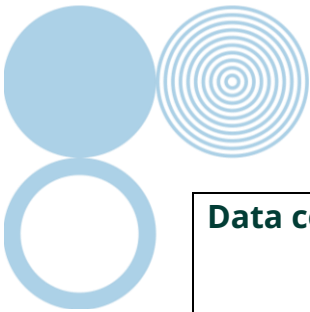




Glossary of Terms

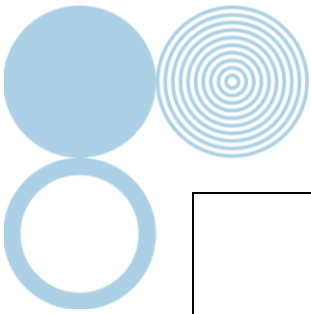
Term	Definition
Access request	A request made by an individual under Article 15 of the GDPR to obtain from an organisation (amongst other things) confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to their personal data.
Capacity	A person's ability to understand when a decision is being made and the nature and consequences of that decision in the context of the available choices. This includes the ability to understand the information relevant to the decision, retain that information for long enough to make a voluntary decision, use or weigh that information as part of the decision-making process, and communicate their decision. This definition is based on section 3 of the Assisted Decision-Making (Capacity) Act 2015.
Consent	Consent means that a person has clearly agreed to the use of their personal data. The agreement must be freely given, specific, informed, and expressed through a clear statement or action.
Covert surveillance	The use of hidden cameras or recording devices to monitor or record individuals.



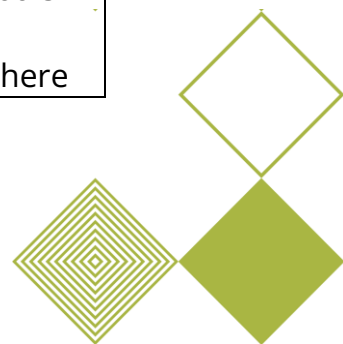


Data controller	A person, company, or other body, which decides the purposes and means of processing personal data.
Data Protection Impact Assessment (DPIA)	An assessment carried out by a data controller of the impact of envisaged processing operations on the protection of personal data where those processing operations are likely to result in a high risk to the rights and freedoms of natural persons.
Data Protection Act 2018 (Access Modification) (Health) Regulations 2022	National regulations which provide for the lawful restriction by a data controller on the right of access to one's health data.
Data subject	An identifiable, natural, living person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, an online identifier or to one or more factors specific to their physical, genetic, mental, economic, or social identity.
GDPR	General Data Protection Regulation (GDPR) lays down rules and obligations relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. A principled piece of legislation which allows organisations of different sizes, and with different objectives, to decide on and devise their own processes and procedures, to meet their respective objectives, once there is adherence to the basic





	principles as set out in data protection law.
Lawful basis	The lawful grounds for processing personal data as set out under Article 6(1) of the GDPR (consent, performance of a contract, legal obligation, vital interests, public task, and legitimate interests).
Legitimate interests	A lawful basis allowing processing of personal data when it is necessary for an organisation's or third parties' legitimate interests, provided those interests are not outweighed by the interests or rights and freedoms of the individual.
Personal data	Any information about a living person where that person is either identified or identifiable.
Processing	Doing something with the personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, consulting, using, disclosing by transmission, sharing/making the data available, aligning or combining, restricting, erasing or destroying personal data.
Public task	A lawful basis allowing organisations to process personal data when necessary to perform tasks in the public interest or exercise official authority. It requires a clear lawful basis in EU or national law for the processing.
Residential care setting	An environment where individuals live and receive ongoing care, support, or supervision, and where





	there is a heightened expectation of privacy.
Safeguarding	Measures put in place to uphold the rights of at-risk adults (including data protection rights), support their health and well-being, protect from harm and reduce risk of harm, and empower at-risk adults to protect themselves and their rights.
Surveillance	The monitoring or observation of individuals through the use of cameras or recording devices.
Technical and organisational measures	Security controls, required under Article 32 of the GDPR to protect personal data against unauthorised access, loss, or destruction.
Vital interests	A lawful basis allowing organisations to process personal data, where it is necessary to protect the vital interests of an individual.





Introduction

The use of video monitoring technologies such as closed-circuit television (CCTV) involves the processing of personal data and therefore falls within the scope of data protection law. Recorded images or recorded video footage that identifies or could reasonably identify an individual, constitute personal data.

This guidance is intended for organisations operating residential care settings where people live and receive care or support. Where these organisations determine the purposes and means of processing personal data through CCTV, they act as the data controllers and are responsible for ensuring that such processing complies with the requirements of the GDPR.

These organisations include, for example, mental health residential services, nursing homes, residential centres for people with disabilities, and special care units. These settings are characterised by ongoing responsibilities of care, support, or supervision, and by the presence of individuals who may be at-risk or dependent.

In such environments, CCTV may be proposed in response to concerns relating to safety, protection, wellbeing, safeguarding, or the investigation of specific incidents. However, CCTV is a highly intrusive form of processing, particularly in environments that function as a person's home, place of care, learning environment, or place of work. The aim of this guidance is to highlight the additional considerations to be taken into account in these settings.

This guidance is provided by the DPC as a guide to help data controllers operating in residential settings to comply with the laws on data protection, and was developed in collaboration with the Mental Health Commission and can be read in conjunction with that organisation's Code of Practice on Digital Monitoring Technologies. Please note that the DPC's guidance does not constitute legal advice.



Heightened expectations of privacy

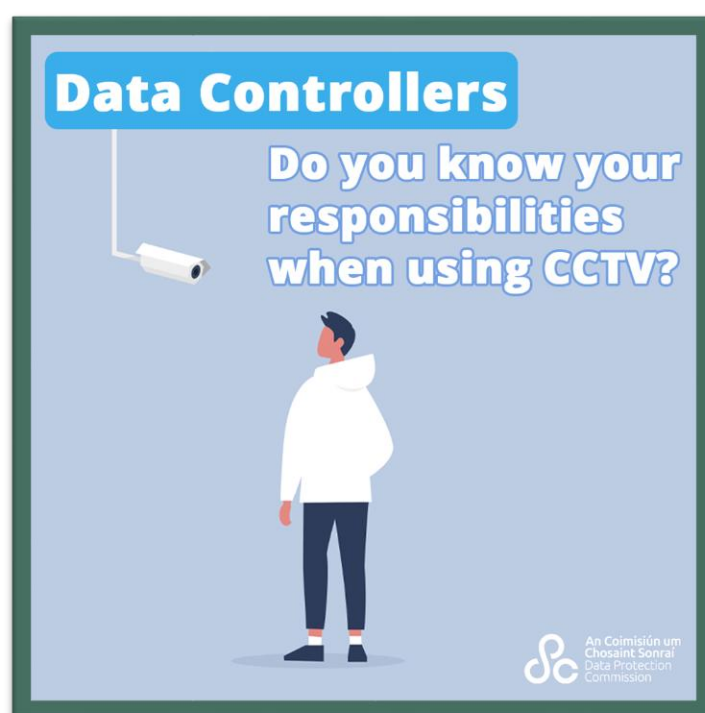
Residential care settings may become a person's home, whether on a permanent or temporary basis. Expectations of privacy are therefore significantly higher than in public or commercial areas.



Although residential care settings may become a person's home, they are not a private household. As a result, these organisations cannot rely on the household exemption under Article 2(2)(c) of the GDPR and must comply with the requirements of the GDPR.

CCTV generally should not be installed in areas where individuals would reasonably expect a higher degree of privacy, such as bedrooms, bathrooms or toilet facilities, changing areas, and therapy, counselling, or treatment rooms.

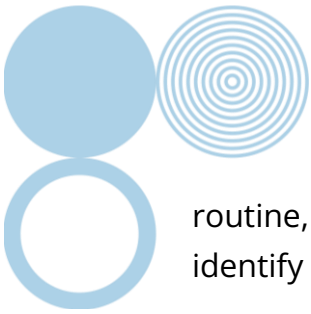
Bedrooms and bathrooms are among the most privacy-sensitive spaces. The threshold for justifying CCTV in such spaces is extremely high. Please see our [CCTV Guidance for Data Controllers](#) which address these issues at pages 21-27.



Purpose of processing personal data using CCTV

Where CCTV is being considered, organisations must clearly identify and document the specific purpose or purposes for which personal data will be processed. CCTV should not be adopted as a





routine, precautionary, or convenience-based measure. It is important to identify the purpose or purposes at the outset, before the processing begins.

As required by the GDPR, organisations must be able to demonstrate that the use of CCTV is necessary and proportionate to achieve a specified, explicit, and legitimate purpose.

Necessity and Proportionality

Necessity requires more than a general concern or a belief that CCTV may be helpful or reassuring should an issue arise.

Organisations must be able to demonstrate that a real and specific issue exists that cannot reasonably be addressed through less intrusive means.



Before deciding to deploy CCTV, organisations should consider alternative measures, such as adjustments to staffing levels or supervision or, changes to care or support arrangements, access controls or alarms, training, or other safeguarding interventions.

The use of CCTV should be clearly linked to addressing an identified issue and should not be relied upon as a substitute for appropriate care, staffing, supervision, or engagement.

Where CCTV is considered necessary, its use must also be proportionate. This may include, ensuring that:

- only the minimum number of necessary cameras to achieve the stated purpose are used,
- monitoring is limited to specific locations and time periods,
- the scope, functionality, and duration of monitoring are clearly defined,
- monitoring does not go beyond what is required to achieve the stated purpose, and



- 
- appropriate retention periods and security measures are in place for any footage capture

Lawful basis

It is important for data controllers to correctly identify their lawful basis for the processing of personal data. Organisations operating CCTV act as data controllers and must identify a

lawful basis for processing **before** any CCTV system becomes operational.

Without a lawful basis, there is no justification for its processing of personal data and this processing is therefore unlawful and in contravention of data protection law. Article 6 of the GDPR sets out a finite list of six lawful bases for the processing of personal data which are: consent, contract, legal obligation, vital interests, public task, or legitimate interests.



In residential care settings, reliance on consent for the processing of personal data is generally inappropriate due to the power imbalances and dependency relationships which often exist. In such circumstances, consent is unlikely to be freely given and may be difficult or impossible to refuse without consequence.

Depending on the circumstances, organisations are more likely to rely on the public task (where permitted by law), legitimate interests or vital interests as the lawful basis for using CCTV. The appropriate lawful basis will depend on the specific purpose of the processing.

Where reliance is placed on public task, the processing must be necessary for the performance of task carried out in the public interest or in the exercise of official authority vested in the controller, where permitted by EU or national law.

Where reliance is placed on legitimate interests, the legitimate interest must be current and real; it cannot be fictitious or speculative. Organisations relying on legitimate interests must carry out and document a legitimate interest assessment. This should assess:

- the nature of the interest being pursued,
- whether it is necessary to process personal data in this way in order to achieve the identified legitimate interest, and



- whether those interests are overridden by the impact on individuals own interests, rights and freedoms.

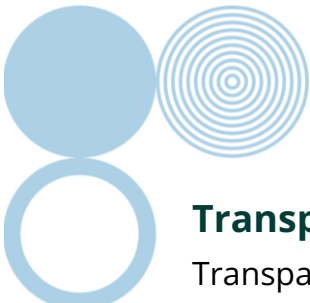
Where reliance is placed on vital interests, the processing must be necessary to protect the vital interests of an individual. This lawful basis is likely to apply in emergency situations, where the processing is necessary to protect someone's life or prevent serious harm.

Where CCTV also captures employees, organisations should consider whether the identified lawful basis is appropriate in the employer-employee relationship and for the specific purpose for which the footage is processed.

Particular weight must be given to the presence of children or other at-risk individuals.

Further information on the lawful bases for processing personal data is available in the DPC's [Guidance on Legal Bases for Processing Personal Data](#).





Transparency

Transparency is a core principle of data protection law under Article 5 of the GDPR and is particularly important in residential care settings, where individuals may have limited ability to understand, avoid, or challenge the use of video monitoring.



Organisations must ensure that clear and accessible information is provided about the use of CCTV, including:

- the identity of the data controller;
- the purpose of CCTV;
- the areas under surveillance;
- who operates the system and who may access footage;
- how long footage is retained;
- whether footage may be disclosed to third parties; and
- how individuals can exercise their data protection rights.

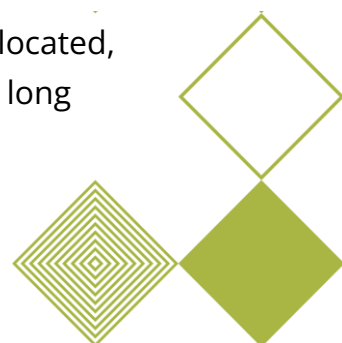
In these settings, transparency will generally require more than signage alone. Information should be provided in a format that is accessible and appropriate to the needs, capacity and level of understanding of those affected.

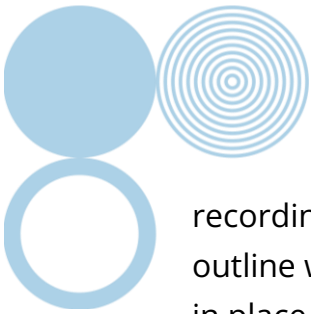
CCTV policy and signage

Organisations using CCTV in residential care settings should have a clear, written policy setting out how the system operates and the safeguards that apply. This helps ensure that CCTV is used consistently, only for its intended purpose, and in a way that people can understand.



The policy should explain why CCTV is being used, where cameras are located, who is responsible for the system, who has access to the footage, how long





recordings are kept, and how individuals can exercise their rights. It should also outline when footage may be shared with third parties and what measures are in place to protect it from unauthorised access or misuse.

The policy should be available to residents, service users, parents or legal guardians, staff, and others who may be affected. It is particularly important that information is provided in a way that people can reasonably understand, taking account of age, capacity, and communication needs.

Clear signage is also an essential part of transparency. People should normally be informed that CCTV is in operation before they enter an area under surveillance. Signs should be placed in clearly visible locations, such as at entrances and within areas captured by cameras, and should be easy to read and understand.

At a minimum, signage should indicate that CCTV is in use, identify the organisation responsible for the system, and explain how further information can be obtained. However, signage alone will not usually be enough in residential care settings. Organisations should also provide more detailed information through policies, privacy notices, or where applicable, on their website.

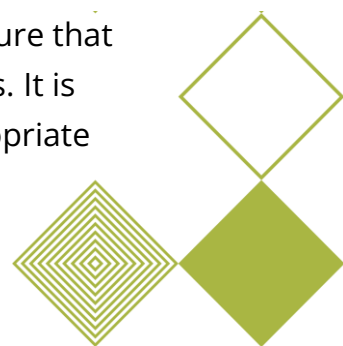
Live-view observation cameras

Some camera systems may only be used to provide a live feed and not record or store footage. Where footage is not being recorded or retained, the use of live-view monitoring does not involve the processing of personal data and data protection obligations do not apply.



However, organisations should clearly inform individuals whether the cameras are being monitored live only or whether that footage is also being recorded or stored.

Where live-view monitoring is used, organisations should ensure that appropriate technical and organisational measures are in place to ensure that staff members do not record footage using official, or personal devices. It is recommended that staff with access to live feeds should receive appropriate





training and access should be limited to those who require it for their role. Additionally monitors for viewing live CCTV should not be placed in, or visible from, publicly accessible areas.

Where live-view monitoring can be accessed remotely, organisations should consider whether this is necessary and have clear policies on remote access. The use of personal devices to access live feeds should only be permitted where it is necessary, authorised and supported by appropriate security measures.

Covert video surveillance

Covert surveillance refers to the use of cameras of which individuals are not aware. Since it involves recording individuals without their knowledge, covert surveillance is highly intrusive and will only be appropriate in rare and exceptional circumstances.



Further information on the use of covert video surveillance is available in the DPC's [Guidance on the Use of CCTV for Data Controllers](#).

Other monitoring technologies

Some residential care settings may also use other monitoring technologies, including but not limited to, smart devices, sensors and wearable technologies. The use of these technologies is likely to involve the processing of personal data and therefore the data protection law continues to apply.



Where technologies include AI-enabled features, organisations should ensure they understand and comply with any additional legal obligations that may apply, including under data protection law.

Before introducing other monitoring technologies, organisations should carefully assess whether their use is necessary and proportionate, and whether less intrusive measures could achieve the same objective.





Technical and organisational measures

Organisations must implement appropriate technical and organisational measures to ensure CCTV systems are secure and controlled. These may include restricting camera placement and angles, avoiding continuous monitoring, disabling audio, applying strong access controls, providing staff training, logging access to footage, establishing clear procedures for disclosure and deletion, and putting safeguards in place to prevent unauthorised secondary use.



A lack of appropriate safeguards may increase the risk of CCTV being used beyond its original and intended purpose.

Rights of individuals

Individuals are data subjects for the purposes of data protection law and all data subjects have rights under Articles 12-22 of the GDPR, though those rights are not absolute. The use of CCTV usually engages a number of rights for individuals whose personal data is captured in footage.



Requests may be made by individuals themselves, parents or legal guardians acting on behalf of a child, or those with legal authority to act on behalf of the data subject.

Organisations must have clear procedures in place for handling rights requests. This includes: identifying when a request was made, confirming the identity of the requester (when required), verifying any authority to act on another person's behalf, locating relevant footage, protecting the data rights and privacy of others captured in the footage, and responding within required timeframes, normally within one month of receipt of the request.

For instance, responding to an access request usually involves providing a copy of the footage in video format. Where other individuals appear in the footage, the organisation needs to consider whether the release of the footage would adversely affect the rights or freedoms of third parties who may also appear in the footage.



The Right of Access to personal data which is medical data is further specified by the Data Protection Act (Access Modification) (Health) Regulations 2022 (S.I. No. 121/2022). This is especially important for CCTV footage in mental health residential settings but applies to all data controllers. Under these regulations the organisation must assess if releasing the CCTV footage would cause serious harm to the physical or mental health of the data subject. If the organisation deems that it would cause such harm, then it may restrict releasing the CCTV footage by relying on the exemption provided for in the Health Regulations. Where access is restricted, the organisation must respond to the individual's request, which should include an explanation of the restriction and their right to make a complaint to the DPC.

Disclosure of CCTV

CCTV footage in residential care settings may, in certain circumstances, be sought by third parties, who have a lawful basis or legal authority to request it. Requests may arise for reasons including, safeguarding or child protection concerns, investigation of alleged criminal or regulatory breaches, or legal proceedings.



Any disclosure must be approached with particular care. Disclosure is not automatic and must have a clear legal basis, be necessary and proportionate, and be limited to what is strictly required for the specific purpose.

Before disclosing CCTV footage containing personal data, organisations should consider:

- the purpose of the request
- the legal basis relied upon
- whether disclosure is necessary
- whether disclosure can be limited
- the impact on the rights and interests of other individuals captured in the footage





Where disclosure is justified, it must be provided securely and decisions should be clearly documented.

Data Protection Impact Assessments (DPIAs)

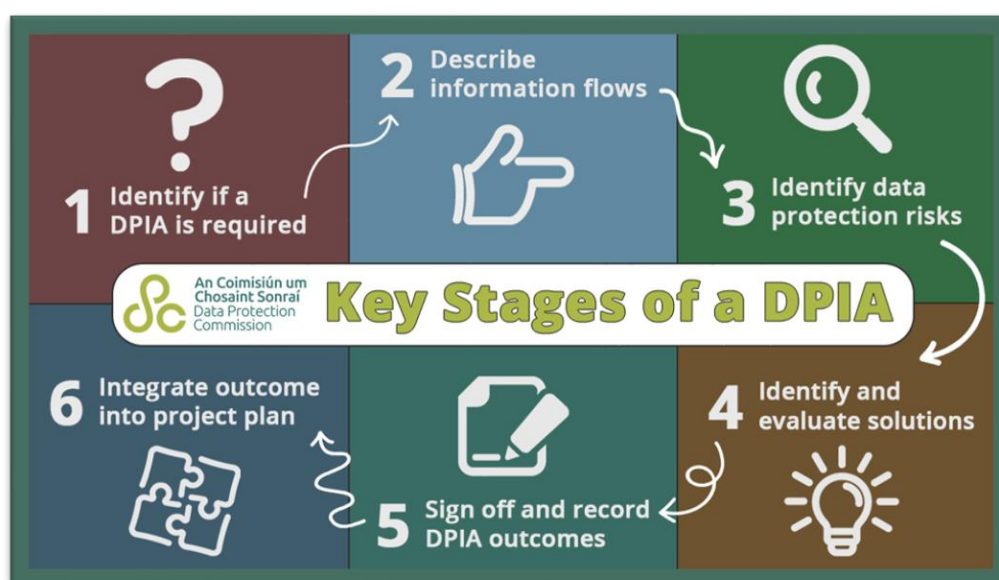
CCTV in residential care settings and similar settings will almost always require a [Data Protection Impact Assessment \(DPIA\)](#).



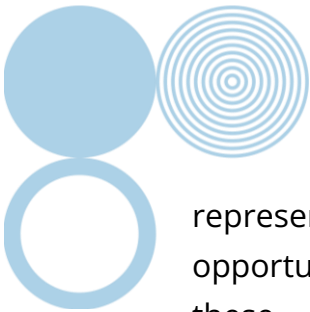
A DPIA assesses the principles of necessity and proportionality, lawful basis for processing, legitimate interests (where applicable), and risks to the individuals affected. It should be used as a genuine decision-making tool, rather than a tick-the-box exercise.

In some cases, the outcome of the assessment may be that the proposed use of CCTV should not proceed, particularly where risks to individuals' dignity or wellbeing cannot be sufficiently mitigated.

Organisations may use the DPIA template provided in the [Adult Safeguarding Toolkit](#), adapted as appropriate. Organisations may also find it helpful to refer to the CCTV checklist contained in the DPC [Guidance on the Use of CCTV](#) as an aid when considering the data protection implications of installing CCTV.



Where appropriate, it can be beneficial as part of the DPIA process to consult with relevant stakeholders, in particular those who will be affected by the processing. In the context of the deployment of CCTV in residential care settings, this might include residents, or their advocates, or staff members or their



representative bodies. The purpose of this is to provide stakeholders an opportunity to express concerns regarding risk, and an opportunity to address these.

Engagement can assist in identifying risks, understanding reasonable expectations of privacy, exploring less intrusive alternatives, and informing assessments of necessity and proportionality.

Ongoing review

The use of CCTV and the DPIA should be kept under regular review to ensure it remains necessary and proportionate. Where the original justification no longer applies, the processing of personal data by way of CCTV must stop immediately.

