THE ALZHEIMER SOCIETY of IRELAND

CCTV Policy 2024

Document Reference No: CCTV2	**Developed by:** ASI Data Protection Officer
Version No.: 2	**Document Approved by:** Senior Management Team (SMT)
Approval Date: August 2024	**Responsibility for implementation:** ASI Senior and middle management at ASI locations nationwide. ASI Data Protection Officer. ASI Estates Manager.
Revision Date: August 2027	**Responsibility for review and audit:** ASI Data Protection Officer. ASI Estates Manager.

Table of Contents

1. Introduction

The Alzheimer Society of Ireland (ASI) is a registered charity in the Republic of Ireland (RCN 20018238) and a company limited by guarantee. This policy sets out the actions and procedures which must be followed to comply with data protection law in respect of the use of Closed-Circuit Television (CCTV) surveillance systems installed and/or managed by The Alzheimer Society of Ireland (ASI) at a number of locations nationwide.

All personal data processed by ASI is protected by Regulation 2016/679/EU, the General Data Protection Regulation (GDPR), in addition to the legislation that transposes this into Irish law, the Data Protection Act 2018. Any person or organisation that collects and processes the personal data of individuals is considered a "data controller". For this reason, any usage of a CCTV system must be considered in the context of the legal obligations imposed on data controllers and implemented in accordance with the principles of data protection.

The use of CCTV systems has expanded exponentially in recent years, due to the increased affordability and sophistication of technology. CCTV systems have legitimate uses in securing premises, supporting workplace safety management, and aiding in the prevention and detection of crime. However, unless CCTV is used proportionately, it can give rise to legitimate concerns of unreasonable and unlawful intrusion into the data protection and privacy rights of individuals and that excessive monitoring or surveillance may be taking place.

All footage or images containing identifiable individuals captured by CCTV systems are personal data for the purposes of data protection law. Where processes are used to obscure or de-identify individuals from CCTV footage, the footage or images are still considered personal data if it is possible to re-identify the individuals. Further, if footage or images are initially captured in an identifiable form and then irreversibly de-identified, data protection law will still cover the processing up to the point of anonymisation.

CCTV systems are located at a majority of ASI care locations nationwide. However, ASI is the data controller of only a small number of these systems. ASI often occupies properties as a tenant or licensee. If such a property is equipped with a CCTV security system ASI had no role in its installation and no role in its ongoing management. In such a circumstance ASI is not the data controller of that particular CCTV system.

1. Purpose

The purpose of this policy is to provide a framework for ASI's utilisation of CCTV at a number of the charity's service locations around the country.

This document supplements the ASI Data Protection Policy. It must also be considered alongside other relevant documents such as the ASI Data Retention & Destruction Policy, the ASI Subject Access Request Policy, the ASI Procurement policy and ASI IT policies.

It is also necessary to consider the transparency requirements of the GDPR as data subjects must be provided with information on how their data is being processed, and very specifically so in relation to CCTV. Therefore, this policy is made publicly available on the ASI website. After reading this policy individuals should be able to identify the range of issues relevant to the use of CCTV at ASI locations.

3. Scope

This policy covers all ASI employees, service users, carers, volunteers, contractors, visitors, and any other individuals whose image may be captured, and their data processed, by an ASI surveillance system. This policy also applies to ASI employees who may be in a position to decide upon the installation and ongoing maintenance of CCTV systems within ASI.

4. Definitions

Personal data is defined under GDPR as information which relates to a living individual (data subject) who is identifiable either directly from the data itself or from the data in conjunction with other information held by ASI. Examples of personal data include, but are not limited to:

- Name, email, address, phone number
- The contents of a service user record or an employee HR file
- Details about donors and their financial contributions
- Photographs and videos generated at an ASI event.
- The contents of complaints or safeguarding incidents received by ASI

Special category personal data is defined under GDPR as information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, also the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning the sex life or sexual orientation of an individual.

Processing is defined under GDPR as any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

5. Roles and Responsibilities

DPO

The role of the DPO is laid out in Articles 37-39 GDPR and in s.88 of the Data Protection Act 2018. The role is primarily one of informing and advising on data protection best practice, including CCTV, and how to effectively implement GDPR and accompanying legislation across the charity. The DPO

interfaces with the public, communicating what data protection law means for individuals and acts as a central liaison with data subjects exercising their rights and with the Irish regulator, the Data Protection Commission (DPC).

Estates Manager (Operations)
The ASI Estates Manager is involved in practical arrangements for the maintenance and servicing of ASI premises, whether owned or leased, including any CCTV system being managed by ASI. The DPO coordinates with the Estates Manager on relevant issues as they arise. The Estates Manager maintains a register of the location of CCTV systems managed by ASI and the contractors they are serviced by.

CEO / SMT
The DPO reports annually to SMT on the salient data protection issues that have arisen. It is possible a particular set of circumstances requires SMT to be notified more swiftly due to their responsibility to coordinate and safeguard the organisation and report to the Board of ASI. The Board's Audit & Risk Committee may also be involved in oversight of the work of the DPO.

Head of Risk
The ASI Head of Risk coordinates internal governance and reporting in respect of the DPO's responsibilities and activities. They also ensure there are systems and structures in place to support the needs of the DPO to carry out their role. The DPO initially escalates any potentially concerning data protection risks to the Head of Risk.

Line Managers
Local service managers at ASI care locations have a key role in the implementation of this policy. They must always make sure they are aware of whether their location has CCTV installed, and if so, whether ASI manages that system.

Even if a third party is the data controller of the CCTV system i.e. landlord, it is nevertheless important that local service managers are happy there is adequate signage so ASI employees, volunteers, service users and families are aware there is a CCTV system on the premises. If signage is inadequate at a leased location, please contact the ASI DPO for further advice.

If a local service manager is tasked with managing an ASI CCTV system at a service location, then this must be conducted in line with this policy. Local line managers should notify the ASI DPO if there is any change to the CCTV system in place so a review can be carried out.

If local managers need support in relation to CCTV compliance, they should contact the ASI DPO. All line managers across ASI must implement this policy and ensure the staff or volunteers they manage are fully aware of, and understand, this policy.

HR / Learning & Development
ASI HR informs all employees about their responsibilities to implement all relevant policies across the charity. Any person who does not comply with this policy shall be liable for disciplinary proceedings

up to and including dismissal. Data protection training materials are provided by the DPO with support and administration from ASI Learning & Development.

Employees & Volunteers
Employees & volunteers must be fully aware of, and understand, this policy. If they have any concerns about the failure of a particular ASI location to fully comply with this policy they should swiftly bring this to the attention of their line manager or directly to the ASI DPO. All employees and volunteers are expected to comply with this policy.

6. Data Protection Law & CCTV

6.1 The Purpose of CCTV

The principles of data protection require that personal data shall be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes". Personal data should not be collected on a 'just-in-case' basis, but only where there is a clearly identified purpose.

This clarity of purpose ensures that data controllers, and their employees, understand why personal data are being collected and processed. It can also serve to address the concerns of individuals when they understand the purpose for which their personal data are being processed. The first step to implementing the use of CCTV is to identify clearly the purpose or purposes for doing so.

The purpose for installing CCTV can be varied and such a system will often be installed for more than one purpose. **In ASI the following purposes for installing and maintaining CCTV systems at a number of locations are:**

- Ensuring security of the premises and assets
- Prevention and detection of crime or disorder
- Apprehension and prosecution of offenders
- Provision of evidence in criminal proceedings or defence of legal claims
- Maintaining health & safety standards for service users, visitors and employees
- Staff monitoring

6.2 The Legal Basis for Processing

As with any processing of personal data, the recording of identifiable images of persons must have a legal basis under the data protection legislative frameworks. Having identified a purpose, or purposes, for installing CCTV, the data controller which installs a CCTV system must also identify an appropriate legal basis for the processing of personal data that will take place.

ASI utilises the legal basis of legitimate interest for CCTV processing. The charity is utilising this technology to protect its property and assets and also to maintain the safety of persons using ASI buildings and their environs.

ASI acknowledges that such legitimate interests provide a legal basis for the processing of personal data, provided that the interests of ASI are balanced with and not overridden by those of the individuals whose personal data are being processed (Article 6(1)(f) GDPR).

ASI is satisfied that it can demonstrate at the relevant ASI locations utilising CCTV that it is genuinely in ASI interests to do so, that it is necessary to achieve the identified purposes, and that it does not have a disproportionate impact on the individuals whose personal data is being processed.

6.3 Necessity and Proportionality

A data controller must be able to justify the use of a CCTV system as both necessary to achieve their given purposes and proportionate in its impact upon those who will be recorded. The data controller must be able to demonstrate why the use of a CCTV system is necessary for the purpose(s) concerned. Proportionality means that any processing of personal data must be measured and reasonable in terms of its objectives.

ASI has decided that utilising CCTV is a necessary and a proportionate measure to protect its premises at several locations across the country. As a charity, resources are not generally available to hire security staff. Some locations are away from residential areas meaning there is no presence in the vicinity overnight. Professional installers area always used to complete the works. All decisions taken during the installation of CCTV systems, e.g. position and number of cameras, the area captured, recording settings, aim for data minimisation with the least intrusion possible on third parties.

ASI is cognisant that staff monitoring using a CCTV system should only occur in certain circumstances. Consideration is given to employees, visitors or service users who may be affected by the deployment of internal CCTV cameras which may result in more intensive monitoring of individuals. ASI Operations may decide that such monitoring is necessary and proportionate for maintaining health & safety standards during times of service provision. ASI HR may decide footage is relevant in a staff disciplinary context. In such circumstances it is vital that clear and compliant signage informs all affected individuals of the presence of the CCTV cameras.

ASI does not place any CCTV monitoring in staff canteens or restrooms, where individuals have a greater expectation of privacy. No DPIA has been carried out on the use of CCTV by ASI but the charity is not engaged in any systematic monitoring of publicly accessible areas on a large scale. Neither is the data of children regularly captured by ASI installed cameras. Any new CCTV system being install by ASI will adopt a privacy by design & default approach to ensure data protection risks are prioritised at the commencement of the project. Despite ever advancing technology such as increased focus or zoom lens capabilities, ASI confines data processed to only what imagery is necessary to achieve the required purpose. ASI does not utilise, but is cognisant that use of, any facial recognition software is

considered biometric data processing which utilises special category personal data. This means it is more sensitive processing than regular use of CCTV systems requiring specific considerations.

6.4 Transparency and Accountability

The principle of transparency means that individuals have a right to be informed about the processing of their personal data (Art. 5, 12, 13, 14 GDPR). Notification of CCTV usage can usually be achieved by placing easily read and well-lit signs in prominent positions. A sign at all entrances will normally suffice indicating the purpose of the CCTV system and the identity and contact details of the data controller. A person whose images are recorded by a CCTV system must be provided with, either directly or in a way the individual can easily access, at least the following information:

- The identity and contact details of the data controller
- The contact details for the ASI DPO
- The purposes for which data are processed
- The purpose and legal basis for the processing
- Any third parties to whom data may be disclosed
- The security arrangements for the CCTV footage
- The retention period for CCTV footage
- The existence of data subject rights and the right to lodge a complaint with the DPC

It is the responsibility of each data controller to determine the most appropriate way to transmit the required information, considering the audience which is intended to receive it.

In terms of the principle of accountability, the GDPR requires data controllers to be responsible for compliance with the principles relating to the processing of personal data, but also be able to demonstrate that they are compliant. ASI maintains a record of all of the charity's data processing activities and includes CCTV systems on processing carried out by ASI Operations at a number of service locations.

6.5 Security of Data

When a data controller installs a CCTV system, due consideration must be given to the safe storage of personal data and the implementation of appropriate security measures. Data controllers are obliged to implement technical and organisational measures to ensure that personal data is kept secure from any unauthorised or unlawful processing and accidental loss, destruction or damage.

The DPC recommends that for CCTV systems, appropriate security measures can include restricting access to footage and the use of encryption and password protection for devices storing CCTV footage. Generic or shared passwords should always be avoided in order to reduce the risk of inappropriate use of the system occurring and going undetected. The storage medium should be maintained in a secure environment and the use and regular review of an access log is one example given on how assurances can be provided that only authorised personnel have access to and may view the footage.

Some CCTV systems allow footage to be accessed remotely, via mobile phone for example. Remote access to CCTV cameras, by whatever means, is becoming more frequent with advances in technology. Such technology is helpful in terms of providing security monitoring of an empty building at night or at weekends. However, controllers utilising remote access must consider any additional risk of unauthorised disclosure which may arise from such functionality. Further potential concerns arise when the remote access occurs around manned workspaces where staff could perceive that their work performance is being monitored on a live basis.

ASI has considered the DPC advice on this issue and has applied suitable security safeguards at all service locations equipped with ASI CCTV systems. The technology is not standardised throughout these locations so each is addressed on a standalone basis. Local service management have been trained in how to securely operate their CCTV system and support is provided to them if a problem arises.

6.6 Data Processors

CCTV systems are often managed and maintained by third party contractors on behalf of data controllers. Security companies that place and operate cameras on behalf of clients may be considered "data processors". They process personal data under the instruction of data controllers (their clients), with a contract in place between the Parties.

Data protection law places a number of obligations on data processors. These include having appropriate security measures in place to prevent unauthorised access to, or unauthorised alteration, disclosure or destruction of, the data, in particular where the processing involves the transmission of data over a network, and against all unlawful forms of processing.

This obligation can be met by measures such as having appropriate access controls to image storage or having robust encryption where remote access to live recording is permitted. Staff of the security company must be made aware of their obligations relating to the security of data.

ASI has contracts in place with all relevant security companies that service and maintain ASI CCTV systems. The agreements contain details on what the security company may do with the data, what security standards should be in place, and for how long the data should be retained. A register of all security companies that process ASI CCTV data is maintained by ASI.

6.7 Retention of CCTV Data

Data protection law requires that personal data should be retained for no longer than is necessary to achieve the identified purpose (or purposes) for which it is processed. The law does not define specific retention periods.

However, specific advice is available from the regulator on the issue of how long to retain CCTV recordings. The DPC advises that retention for 30 days would generally appear to be "a reasonable proportionate and balanced" length of time. In any event, the retention period should be the shortest period necessary to achieve the purpose for which the system was installed and should allow the controller enough time to review any footage as necessary before deleting the data.

The DPC notes there is a possibility the data controller could face a personal injuries action related to footage they have deleted after 30 days but that civil litigation legislation ensures this will not negatively affect defence of the action if the Plaintiff did not notify the Defendant within 30 days.

The DPC further notes it is difficult to justify retention beyond one month, except where the images identify an issue – such as a workplace incident, a fall by a service user, a break-in, theft or assault – and is retained specifically in the context of the investigation of that issue. Where footage has been identified that relates to such a specific incident a longer period may be justifiable for the section of footage concerned. This footage should be isolated from the general recordings and kept securely for the purposes that has arisen. **Local service management must liaise with the ASI DPO and potentially other senior and middle management, to ensure this process of retaining important footage is conducted correctly and securely.**

Where a CCTV recording system or device has a default retention period the settings should be reviewed by the data controller and set at their own assessment of what is the appropriate retention period.

7. CCTV in the Workplace

While employers may have legitimate purposes for installing CCTV, employees also have legitimate expectations that their privacy will not be intruded upon disproportionately. CCTV recording should be avoided in areas where employees have an increased expectation of privacy such as break rooms, changing rooms and toilets.

Where possible, cameras should be focused upon areas of particular risk, for example, at entrance walkways where trips could occur, at rear windows vulnerable to a break-in, or external environs of the property where observation is difficult and unauthorised access could occur.

Employees should be given clear notification that CCTV monitoring is taking place and informed as to where and why it is being carried out. ASI has clearly outlined that staff monitoring is a purpose of ASI CCTV systems as this purpose will often overlap with ASI's requirement to provide a safe environment for service users, carers or other members of ASI staff, another stated purpose of ASI CCTV systems.

In addition, situations may arise where ASI, as an employer, needs to use CCTV footage to investigate an allegation of gross misconduct or other disciplinary matter. The DPC advises that this course of action by an employer may be legitimate where it is carried out strictly on a case-by-case basis and is justified based on necessity and proportionality to achieve the given purpose.

In such a circumstance, the employer must be able to demonstrate why the use of CCTV is necessary to provide evidence in a disciplinary matter, and that their access and use of CCTV footage is proportionate and limited in scope to the investigation of a particular matter. In such cases, the rights of the employee and their expectation of privacy will not be seen as overriding the interests of the employer, and the employee's data protection rights should not be seen as presenting a barrier to the investigation of serious incidents.

Some ASI staff do not work at one specific ASI location but rather in the community. These ASI staff visit the homes of persons with dementia and their families. ASI has no control over whether any home has a CCTV camera or cameras in situ. Any domestic CCTV system which operates in a way that captures images of people only within the perimeter of the CCTV operator's own property means it is not subject to data protection law due to the household exemption in that law.

ASI does ask each family that engages ASI for regular home care to confirm whether or not there is such surveillance in place. It is also reasonable for ASI to ask whether any cameras on the property provide a recording and/or a live feed. If ASI has confirmation that cameras are present, then relevant ASI care staff should be made aware by their line management that cameras are in situ.

The use of recording mechanisms to obtain data without an individual's knowledge is generally unlawful. Covert surveillance is normally only permitted on an exceptional case-by-case basis where the data is kept for the purposes of preventing, detecting or investigating offences, or apprehending or prosecuting offenders. The actual involvement of An Garda Síochána or other prosecution authorities for potential criminal investigation or civil legal proceedings being issued, is required.

8. Disclosure of CCTV to Third Parties

On occasion, a data controller may be asked to disclose CCTV recordings to third parties for a purpose that may, or may not, be for a purpose which they were originally obtained. This may arise, for example, where a request is received from An Garda Síochána or another law enforcement body to provide footage to assist in the investigation of a criminal offence that may not necessarily be relevant to the data controller.

In any such circumstance, it is recommended that requests for copies of CCTV footage should only be acceded to where a formal written request is provided to ASI stating that An Garda Síochána (or other law enforcement body) is investigating a criminal matter. For practical purposes, and to expedite a request speedily in urgent situations, a verbal request may be sufficient to allow for the release of the footage sought. However, any such verbal request should be followed up with a formal written request. A record of all Garda Síochána requests must be maintained by ASI so local service management must inform the ASI DPO who will record the incident and provide advice, if required.

A data controller may also be requested to provide CCTV footage to a non-law enforcement third party to investigate an incident. In such cases, the same assessment procedure as applied for the original purpose should be applied to the new purpose to determine if it can be justified in the pursuit of a

genuinely legitimate interest of the data controller or another party. Such eventualities will need to be assessed on a case-by-case basis. The legitimate interests of a third party do not oblige ASI to disclose CCTV footage but may permit such disclosure subject to assessment. A requesting third party should never be given direct access to the ASI CCTV system. Any copy recording will be organised and provided by ASI with any cost borne by the requesting party.

9. Providing Access to Data Subjects

Data protection law provides individuals with a right of access to, and a copy of, their own personal data. This right extends to any individual whose identifiable image has been recorded by a CCTV system. When a data controller receives a request from an individual to access CCTV data ASI will process any such Data Subject Access Request submitted by an individual as per the relevant ASI policy document. The ASI DPO is responsible for liaising with the individual exercising their right of access.

If the requested recording has already been deleted by the date the request is received, the defined retention period having expired, the individual should be informed that the footage no longer exists. If an access request has been received, the footage should not be deleted until the request has been fulfilled.

Responding to an access request usually involves providing a copy of the footage in video format, as well as providing detailed information on the legal basis and purpose for the filming, and any disclosures that may have been made. Where the footage is technically incapable of being copied to another device, or in other exceptional circumstances, it may be acceptable to provide picture stills as an alternative to video footage.

Where images of parties other than the requesting data subject appear on the CCTV footage the data controller needs to consider, on a case-by-case basis, whether the release of the unedited footage 'adversely affects' the rights or freedoms of the third parties. Where necessary, measures may include pixelating or otherwise de-identifying the images of other parties before supplying materials to the requester. Alternatively, the data controller may seek the consent of other parties whose images appear in the footage in order to release an unedited copy containing their images to the requester.

10. Data Breach Procedure

All ASI staff or volunteers are required to report any actual, suspected or potential breach of CCTV data as they would with any other breach of personal data within ASI. The handling of any breach would be as per the relevant ASI policy document. Any concerns that ASI CCTV footage have been inappropriately accessed, damaged or removed from ASI premises must be reported swiftly to the ASI DPO.

11. Checklist for Service Locations with ASI CCTV

11.1 Equipment and Installation

ASI must give careful consideration to how it installs and where it locates CCTV equipment in line with guidance issued by the DPC. Local and Regional ASI management must assess the following:

- Are all CCTV cameras located in prominent positions?
- Are all CCTV cameras filming only ASI property?
- Is CCTV footage being automatically recorded?
- Has CCTV recording equipment been configured to retain data for no longer than 30 calendar days?
- Are all CCTV monitoring screens and recording devices positioned out of view of the public and secure from unauthorised access?

11.2 Signage

- Have you erected CCTV signage on all entrance points to the premises and throughout the site?
- Are service users and visitors aware they are entering an area that is covered by CCTV surveillance equipment?
- By law CCTV signage should contain the following information:

✓ Contact details for ASI and the ASI DPO
✓ The purposes of the CCTV system
✓ The legal basis for the processing
✓ Any third parties to whom data may be disclosed
✓ The security arrangements for the CCTV footage
✓ The retention period for CCTV footage
✓ The existence of data subject rights and the right to lodge a complaint with the DPC

- Does your signage contain the above level of detail? If not, please contact the ASI DPO.

11.3 Recorded Images

- Are the images produced by your CCTV system as effective as possible for the purpose for which they are intended?
- Are you confident that all recorded images will be stored securely within the system hard drive, for up to 30 days, after which they will be automatically erased if not needed as evidence?
- If an incident has occurred and evidence may be required, have you swiftly contacted the relevant ASI management and the ASI DPO to inform them that arrangements need to be made to securely save down and store the recorded images?
- Are you aware that such saved images need to be professionally managed with access strictly limited to key senior personnel?

12 . Who to contact

For further information and advice about the use of CCTV within ASI please contact:

ASI Data Protection Officer

- By email: dataprotection@alzheimer.ie
- By post: DPO, Alzheimer Society of Ireland, National Office, Temple Road, Blackrock, Co. Dublin
- Tel: +353 85 8035088 or +353 1 2073800

Comprehensive information on the use of CCTV surveillance systems is available on the website of the Data Protection Commission: www.dataprotection.ie