This policy sets out Amplius's approach to using surveillance technologies (should this be required), including CCTV cameras, detailing safeguard to ensure lawful processing of the data concerned.

CCTV and Surveillance Policy

Document management

Directorate	People and Governance
Policy sponsor	Chief People and Governance Officer,
Policy owner	Director of Compliance and Regulation
Policy author	Assistant/Data Protection Officer

Review process

Approval route	Directors Team
Approved by	Chief People and Governance Officer
Approval date	28 November 2024
Effective	17 December 2024
Review Frequency	Triennial
Review date	28 May 2026
Version number	1.0

CONTENTS

Part 2

Overview

Policy statement

This policy supports Amplius's values and is a commitment to improving lives and supporting colleagues by:

- Amplius is committed to creating an environment that promotes the peaceful enjoyment of colleagues, customers, and the public. This policy outlines Amplius's approach to deploying CCTV and other surveillance technologies in a way that aligns with legal requirements, balancing Amplius's legitimate needs with individuals' privacy rights. It ensures that any personal data captured is protected through appropriate security measures.
- Amplius relies on legitimate interest as the lawful basis for processing CCTV footage, recognising that special category data may occasionally be captured. This policy also reaffirms Amplius's dedication to meeting its legal and regulatory responsibilities, including compliance with the ICO's guidance, and emphasises transparency and accountability in processing personal data.

This policy is a Day 1 provision for Amplius as a newly established company, it is subject to review as we develop and review our policies over the next 18 months.

Scope

The term Amplius incorporates all member companies and subsidiaries.

The policy applies to:

- Customer's, volunteer's, colleagues', former colleagues and third parties
- The policy sponsor is the Chief People and Governance Officer, aligning it with business plans and strategies.
- The Director of Compliance and Regulation owns the policy, ensuring its suitability, implementation, and review; and
- The Data Protection Team is responsible for drafting and updating the policy.

This policy is referred to as the "CCTV policy" throughout

This policy should be read in conjunction with the Data Protection and Confidentiality policy, Subject Access Request Procedure and the CCTV procedure.

The term 'Customers' is used throughout and refers to the following, applied variously, to tenants, residents and leaseholders of Amplius.

Amplius's surveillance is undertaken when a need is identified. Clear signage will be used when surveillance is installed.

Siting and coverage of the CCTV camera(s) will be justified and proportionate to the problem identified as the key reason for the installation.

Covert surveillance may be used in extreme circumstances in conjunction with agencies such as the police.

Amplius does not normally record sound and does so only in ‘exceptional circumstances’ as set out in the Surveillance Camera Commissioner’s CCTV Code of Practice.

The policy does not form part of any colleague’s contract of employment and the policy may be amended at any time.

Part 3

Policy details

Purposes and Grounds for the use of CCTV

CCTV is designed for the prevention and detection of crime.

Amplius will establish a clear justification and need for the installation of CCTV in a particular location, taking into account:

- Establishing the lawful basis for the surveillance
- Proportionality to the identified problem
- Consultation with residents, police, local authorities or other relevant stakeholders
- Other measures that may run alongside or instead of CCTV.
- The legal rights of individuals under relevant data protection legislation
- A completed Data Protection Impact Assessment (DPIA)

Likely problems and reasons for installation will be:

- The detection of anti-social and/or criminal behaviour
- The prevention and detection of unauthorised access to premises
- The prevention and detection of criminal activity within premises

CCTV Signage

Signage will be installed to ensure staff, customers, visitors, and members of the public are aware they are entering an area that is covered by CCTV. The signage will include the Amplius logo and relevant contact details.

Storage, retention and disposal

Recorded images will be stored securely for a maximum of 30 days or in the case of investigations of events, for as long as that investigation or subsequent action takes place. The directions of police or court action will take precedence.

Images will automatically be overwritten after this period.

Access and viewing

Access to CCTV systems will be carried out by authorised staff only with a valid reason. Each view is documented or maintained in audit files in the system.

CCTV footage can be shared with the police, local authorities and colleagues with the appropriate signed and approved authorisation.

All access requests for CCTV footage are recorded in a central register.

Disclosure

Where Amplius is required to share images, the Data Protection Team must authorise all requests.

Maintenance and Compliance

CCTV installations shall be subject to a routine maintenance undertaken by appropriately qualified staff or contractors.

Equality, diversity and inclusion

Amplius recognises that an effective CCTV policy will help to promote and protect the interests of groups outlined within the Equality Act 2010.

Summary of local variations

There are no local variations associated with this policy.

Part 4

Compliance and administration

Legal and regulatory compliance

This policy fully complies with Amplius's legal and regulatory obligations.

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 (DPA)
- Human Rights Act 1998 (HRA) – Article 8 – respect for private and family life
- Regulation of Investigatory Powers Act 2000 (RIPA)
- Protection of Freedoms Act 2012 (POFA)
- Surveillance Camera Code of Practice 2013
- ICO CCTV Code of Practice - 2023

This list is not exhaustive, and policy authors will undertake thorough research and/or seek professional advice to ensure that Amplius meets its obligations and complies with the current and relevant legislation and regulations.

Evaluation, review and performance monitoring

This policy will be reviewed on a Triennial basis to ensure that it remains fit for purpose. A policy review may also be required earlier, in response to internal or external changes for example changes in legislation. Prompt and effective action will be taken where improvements are identified.

CCTV footage requests will be reported quarterly to the Audit and Risk Committee as part of the Audit and Risk compliance update. In addition, monthly reports will be provided to Directors.

Related policies

- Data Protection and Confidentiality Policy
- Safeguarding Adults and Children Policy

Part 5

Appendices

A. Associated documents – Internal procedural documents, colleague use only

- CCTV Procedure - LG

Part 6

Changelog

Amended date	Summary of changes	Version №