CCTV and Visual Recording Systems Policy

1.0 Purpose and scope

This policy provides a framework for Notting Hill Genesis (NHG) when installing/using equipment which could be used for visual surveillance of residents, suppliers, staff, NHG properties and people who visit them.

This policy sets out the legal basis for our use of recording systems, the limits to any recording and best practice.

The policy is based on the requirements of section 13 of the Data Protection Act 2018 and General Data Protection Regulations and has been assessed against both the Information Commissioner's Office (ICO) and Surveillance Camera Commissioner codes of practice and checklist.

The policy applies to all visual recording systems used by NHG such as closed circuit TV systems (CCTV), body worn video (BWV), automated number plate recognition (ANPR), mobile phones, dashcams and so on.

Section 13 and 14 of this policy apply to domestic systems which are not deployed and/or monitored by NHG such as CCTV systems or video doorbells installed by residents to monitor their own properties / rooms within our properties.

The policy does not cover the use of lone working devices such as Alertcom, which may record sound only.

The policy links to our information management suite of policies and is in line with ICO and Surveillance Camera Commissioner codes of practice on CCTV.

2.0 Definitions

Surveillance – means to watch or record. In this instance, surveillance refers to any technology used to record moving images of individuals. Surveillance systems can be:

- staffed (for example, control room where cameras are actively monitored)
- unstaffed (for example, remote CCTV cameras that record and download to a single location, often reviewed in response to an incident)
- operator controlled (for example, body worn video activated by an individual)

- Remote controlled (for example, drones undertaken roof surveys)

Overt surveillance – is where individuals are aware that the cameras are present and that recording is taking place (usually notified through signs or notification from the operator that recording is taking place).

Covert surveillance – refers to a surveillance system that is hidden, where individuals are not notified that they are being recorded. We do not directly undertake covert surveillance. Any covert surveillance of our properties is carried out by police/local authorities.

Intrusive surveillance – covert surveillance of anything taking place in or on residential premises or in a private vehicle which involves the presence of an individual on the premises or in the vehicle, or the use of a surveillance device. We are prohibited from undertaking intrusive surveillance.

Visual recording system – any system which carries out surveillance / visual recording of individuals

'We': Notting Hill Genesis as an organisation.

3.0 Policy statement

This policy ensures that our use of CCTV and visual recording systems complies with data protection legislation and codes of practice, in particular the 12 principles of the Surveillance Camera Commissioner's code of practice:

1. Use of a surveillance camera system (SCS) will always be for a specified purpose in pursuit of a legitimate aim and necessary to meet an identified pressing need.

2. The use of a SCS will take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

3. There will be as much transparency in the use of a SCS as possible, including a published contact point for access to information and complaints.

4. There is clear responsibility and accountability for all SCS activities including images and information collected, held and used.

5. Clear rules, policies and procedures will be in place before a SCS is used, and these must be communicated to all who need to comply with them.

6. No more images and information will be stored than that which is strictly required for the stated purpose of a SCS, and such images and information will be stored for no more than 30 days and deleted in accordance with NHG retention policy once their purposes have been discharged.

7. Access to retained images and information will be restricted and there are clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.

8. SCS operators will consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.

9. SCS images and information is subject to appropriate security measures to safeguard against unauthorised access and use.

10. There will be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports will be published.

11. When the use of a SCS is in pursuit of a legitimate aim, and there is a pressing need for its use, it will be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.

12. Any information used to support a SCS which compares against a reference database for matching purposes will be accurate and kept up to date.

4.0 Technical standards

Any CCTV/visual recording system that we use will meet the technical requirements as set out in Surveillance Commissioner's technical standards and/or other industry standards.

In all cases, footage must be legible, fit for purpose and captured in a resolution sufficient to allow the footage to be used for the purposes set out in the relevant privacy impact assessment (PIA) (see section 6).

5.0 Access management

Each visual recording system/process will have a:

- System owner – the person who is responsible for ensuring that all required PIAs and reviews are conducted, and that the system meets the identified legitimate interests. They will not directly access records but are responsible for making sure the system is used appropriately. This will usually be a manager or above.
- System operator(s) – authorised staff member(s) who can view/share footage in response to incidents/requests. They are not able to alter the location or position of any cameras and any request for access/sharing of footage must be authorised by the system owner prior to footage being obtained from the system.
- System administrator(s) – authorised staff member(s)/contractor(s) who can access the list of cameras/devices used in the visual recording system and ensure that they are working and meeting the technical/security standards. They can action repairs of cameras and arrange for repositioning of devices in response to requests from the system owner. This will usually be facilities management or third-party suppliers.

Where devices are allocated to individual operators – for example, body worn video – a list of the assets used will be maintained showing the asset number,

who it was assigned to, duration and whether any incidents were captured. This asset list is maintained by the system owner.

As part of their employment with us, some staff are issued with mobile phones which are able to record visual images. A list of all devices issued to the business is maintained by IT/mobile phone provider. However, staff only record images using the recording function of their device where there is prior approval from their manager to do so and where the process has been authorised by the system owner.

Staff do not record customers in their homes without the knowledge of the customer as this would constitute intrusive surveillance which we are prohibited from undertaking.

6.0 Privacy impact assessments

The system owner ensures that a PIA is undertaken for all new deployments of visual recording systems used for overt recording. The PIA includes a consultation with all relevant stakeholders. All PIAs are signed off by the system owner, data protection officer via the data protection team) and, the relevant director. The template for PIAs is based on the Surveillance Camera Commissioner's recommendations.

PIAs consider all risks to privacy of individuals and the controls in place to reduce those risks, such as the use of privacy zones to prevent the capture of unnecessary information / unwarranted intrusion on the privacy of individuals.

All PIAs are reviewed on an annual basis by the system owner to ensure that the visual recording system is justified and that the devices used are appropriate to the aims. Any amendments to the system as a result of the PIA are implemented. PIAs are recorded in line with our data protection policy. Compliance with the policy is monitored, as set out in section 11 below.

7.0 Privacy notices

Where visual recording systems are installed, adequate signage will be in place to inform individuals that they are being recorded. Any signage complies with any standards in place at the time, such as those set out by the Information Commissioner and/or the Surveillance Camera Commissioner and include as a minimum the published contact point for access to information and complaints. Signage will be in place before recording begins.

Where the visual recording system is operator controlled, individuals are informed that they are being recorded. As part of the PIA, consideration is given to how this information can be delivered to the individuals subject to the recording – for example, on staff uniforms or via a notice handed to them.

8.0 Security, storage and retention

Footage is retained only for as long as is necessary to fulfil the purposes for which the footage is captured. Footage is not held in the visual recording system for longer than 30 days in the initial instance. The retention period is identified in the PIA.

All footage in the visual recording system and any isolated/extracted footage is retained in a secure environment – for example, it will be encrypted where possible. Any transfer of data from the recording system to the storage system (for example, from mobile phones, via the internet) is also secure.

All footage which is outside of the retention period set is automatically deleted once the retention period has expired, unless the footage has been isolated in response to a request (see Section 9).

9.0 Access to footage

Where access to footage is required for our purposes of investigating an incident, such as theft, insurance claim, or health and safety, the relevant footage is extracted from the system by the system operator and saved to a secure location. Requests for footage are authorised by the system owner. A retention period for the isolated footage is set at this time. The system owner ensures that isolated footage which has expired its retention period is deleted in line with this policy.

Where a request is from a member of the public / member of staff (or via an authorised representative such as a solicitor) for information about themselves, the request is handled in line with our subject access request procedure.

Access to footage by members of the public / member of staff is not provided where the information requested is not their personal data – where it is about another party, property (such as a vehicle) or incident which does not directly involve them – or where disclosure would be subject to an exemption under the Data Protection Act 2018 (for example, schedule 2). In these cases, a request must be made by the appropriate authorised third party.

Where the request is from an authorised third party such as the police or an insurance company, the request is recorded and verified by an appropriate staff member such as the system owner or data protection officer, prior to any footage being released.

All requests for footage are recorded.

10.0 Third-party suppliers

Where visual recording systems are provided by third party suppliers, the system owner ensures that they adhere to this policy with regard to technical standards, access management and retention of footage.

Contracts with suppliers also stipulate the service level agreements for returning footage in response to requests to ensure that legal obligations in respect of subject access requests and third-party requests can be met within the appropriate timescales. All third-party suppliers are approved and authorised by the in-house Procurement Team and selection complies with our Procurement Policy.

11.0 Review, audit and monitoring

The data protection officer (DPO) monitors all privacy impact assessments (PIAs) to ensure that they are reviewed on an annual basis. The DPO also arranges for regular audits to be carried out on all records relating to visual recording systems

including records of requests, asset lists and granting of access rights, to ensure that the policy is being adhered to. Audit outcomes will be presented to the NHG audit committee to ensure any risks associated with use of visual recording systems are managed appropriately.

12.0 Complaints

Where a complaint is received regarding the use of a visual recording system from a member of the public or an authorised representative such as an MP, councillor or solicitor, this is dealt with in accordance with our complaints policy, including the timescale for a response.

Complaints from the Information Commissioner's Office are dealt with by the data protection officer.

13.0 Requests to install an external fixed camera

The use of recording equipment, such as CCTV or smart doorbells, to capture video or sound recordings outside the boundary of a resident's property is not a breach of data protection law.

Where your occupancy agreement requires you to seek permission for a home improvement, you must submit a formal request to your Local Officer to install an external fixed camera system.

13.1 Requests

We recognise that cameras can sometimes be used as a means of coercive control. For that reason, if a resident or member of their household has had an allegation of domestic abuse or anti-social behaviour made against them, we will not grant permission to install a fixed camera.

We will only give permission for external CCTV to be installed if the equipment is for the sole use of crime prevention and detection and home security. Your Local Officer will discuss with you other solutions that could be considered, for example security lighting or a neighbourhood watch scheme.

13.2 Conditions of permission

Fire safety

Requests to install or erect an external fixed camera will be refused if this would compromise the fire safety of the building, for example, by screwing equipment into a fire door.

Positioning

Requests to install an external fixed camera will only be granted where a resident agrees to install the equipment in a position that complies with the provisions of any Data Protection and Privacy regulations. Before granting permission, a resident will be asked to sign a declaration (Appendix 1) whereby they agree to follow surveillance guidance on the Information Commissioners' website.

To avoid any sanction by the regulator, including a fine, it is important the equipment does not view:

- Any other property

- Any public area, such as the footpath, pavement, or road.

Generally, requests to install a camera to a communal wall within a block are likely to infringe the privacy rights of neighbours and will therefore be refused.

Where these conditions have not been met, we will withdraw permission and ask the resident to remove the fixed camera. If a camera is not subsequently removed, this will be a breach of the occupancy agreement. We will therefore take action to remove it and may charge the residents with the costs of removal.

Where our permission to install the equipment is not required but the fixed camera fails to comply with surveillance guidance, we will advise neighbours who are dissatisfied with the fixed camera to make a complaint to the Information Commissioner's Office.

We will recover the costs for repairing any damage caused by the removal of a fixed camera from the resident when the property is vacated.

14.0 Installation of CCTV inside a home

Residents do not need our permission to install CCTV to capture images within the boundary of their private domestic property (including the garden). Data protection laws will not apply, as long as the resident is not capturing images outside of this boundary of their property.

If a system captures images of NHG staff (within the boundaries of a private domestic property), the resident must inform NHG in writing of the installation to ensure NHG staff are aware of the recording.

If the system captures images of people outside the boundary of your private domestic property – for example, in neighbours' homes or gardens, shared spaces, or on a public footpath or a street, data protection laws will apply and the resident will be expected to comply with section 13 of this policy.

14.1 Covert recording of NHG staff

Recording NHG staff within the boundary of a private domestic property without informing NHG or sharing the recordings without their consent could lead to those affected staff claiming damages.

Selling the recordings to third parties or releasing it in public without staff consent could be considered a criminal offence.

15.0 Our approach

In writing this policy we have carried out a diversity and inclusion impact assessment and no adverse impacts were identified. The policy does not involve the use of personal, sensitive information so it has not been necessary to carry out a privacy impact assessment. All CCTV deployments will require individual PIAs to be conducted to identify any specific privacy risks.

16.0 Reference

- Data Protection Act 2018
- General Data Protection Regulation (EU) 2016/679

Document control

Author	Bahzad Brifkani, Data Protection Manager
Approval date	1 July 2020
Effective date	1 July 2020
Approved by	Policy Group
Policy owner	Data Protection Manager
Accountable Director	Director of Health and Safety and Office Services

Version Control

Date	Amendment	Version
June 2018	New Notting Hill Genesis policy created.	1.0
July 2020	New section 13 relating to residents installing CCTV	1.1
August 2020	Paragraph on covert recording added (section 13). Reference to internal procedures added	1.2
November 2020	Clarified on the Policy position on installation of CCTV by a resident	1.3
March 2021	Added appendix 1	1.4
1 February 2024	Statements added to section 13 that make clear NHG's position on video doorbells: residents must seek permission, which will usually be granted where the conditions outlined are met	1.5

Appendix 1

CCTV declaration

Resident/requester's full name:

Full address:

Date of request:

Purpose of request:

I/we

formally request that Notting Hill Genesis (NHG) considers my/our application for CCTV at our address. If NHG agrees to my/our application, I/we agree to keep to the below conditions. I understand that NHG may withdraw permission for personal CCTV use at any time and will do so if I do not keep to any of the below conditions.

I/we agree:

- To ensure that any camera I/we use is only directed at my/our own property which may include my/our home and any gardens which I/we have for my/our sole use. The camera may not capture any part of a public place or any private property owned or resided in by others. This applies even if the camera is not recording.
- That recording that takes place is solely used for the purposes of home security, i.e. The prevention or detection of crime, nuisance or anti-social behaviour on the property.
- That I/we are responsible for the usage of the camera. I understand that the NHG will not be held responsible for inappropriate recording or for the malicious use of recorded material.
- To follow and adhere to the Information Commissioner Office's (ICO) guidance on the use of the domestic CCTV systems in my property.
- To obtain all necessary permissions to carry out alteration work that may be necessary for the CCTV to be installed in line with the tenancy agreement.

That I/we understand that malicious or inappropriate use of CCTV recordings, including distributing recordings of others without their permission, may be a criminal or civil offence and would be a breach of the tenancy agreement. I understand that I may be subject to criminal proceedings or tenancy enforcement action should any evidence of CCTV misuse be received by NHG or the Police.

Resident/requester: Signature: Date:	Staff name: Signature: Date