CCTV Surveillance Policy

If you need any information in a different format, for example large print, Braille, audio file or another language, please email Communications@housing21.org.uk

Version number	4.0
Issue date	June 2023
Review date	May 2026
Board approval required?	No
If yes, date approved by Board	N/A
Author's name and job title	Sonia Hawley, Information Governance Manager and DPO
Policy owner and job title	Annabel Ellin, Director of Audit, Assurance and Governance
Policy Steering Group approval date	May 2023

Summary

The Data Protection Act 2018 (DPA18) and the UK General Data Protection Regulation (UKGDPR) provide individuals with the right to know what personal and special category information is held about them and how it is processed and protected. It also sets out requirements for organisations to adhere to when collecting and processing personal data.

This extends to personal data captured on CCTV. CCTV and other surveillance systems have a legitimate role to play in helping to maintain a safe and secure environment for all our employees, residents, carers, and visitors.

Housing 21 recognise that this may raise concerns about the effect on individual's privacy. Images recorded by surveillance systems are personal data which must be processed in accordance with data protection legislation

and regulation.

This policy aims to set out clear guidance on:

- Employee obligations in the protection and processing of personal data
- Data Controller obligations in the protection of personal data
- Individuals' rights in relation to their personal data

Compliance with this policy is mandatory for all employees. Related policies, privacy guidelines, glossary and terms are available to help you. Any breach of this policy and the related mandatory information governance eLearning training provided to all employees, may result in disciplinary action.

The term 'employee' refers to all Housing 21 employees, including: permanent, fixed term, temporary, Board Members, secondees, third party representatives, agency workers, volunteers, interns, and agents.

In certain circumstances, misuse of information generated by CCTV or other surveillance systems can constitute a criminal offence.

Equality, Diversity and Inclusion

Housing 21 aspires to embed diversity and inclusion within all our organisational activities to enable these principles to become part of our everyday processes.

1.0 CCTV Rationale

1.1 Housing 21 use CCTV surveillance cameras to view and record individuals on (and around) our premises. Surveillance systems means any devices or systems designed to monitor or record images of individuals or information relating to individuals. The term includes CCTV systems as well as any technology that may be introduced in the future such as body worn cameras, unmanned aerial systems and any other systems that capture information of identifiable individuals or information relating to identifiable individuals.

1.2 This policy details:

- Why we use CCTV,
- How we will use CCTV and
- How we will process data recorded by CCTV cameras
- Who we may lawfully disclose CCTV footage to
- How to make a subject access request in respect of personal data created by CCTV.

1.3 This policy covers all employees and may also be relevant to residents and visiting members of the public.

1.4 The policy will be formally reviewed every 3 years, although it may be amended at any time to ensure that it meets legal requirements, relevant guidance published by the ICO and industry standards.

1.5 A breach of this policy may, in appropriate circumstances, be treated as a disciplinary matter. Following investigation, a breach of this policy may also be regarded as misconduct leading to disciplinary action, up to and including dismissal and/or criminal sanction.

1.6 The Information Governance Steering Group (IGSG) has overall responsibility for ensuring compliance with relevant legislation and the effective operation of this policy. Day-to-day management responsibility for deciding what information is recorded, how it will be used and to whom it may be disclosed has been delegated to the Data Protection Officer (DPO). Day-to-day operational responsibility for CCTV cameras use and the storage of data recorded is the responsibility of the scheme manager.

2.0 Reasons for the Use Of CCTV

2.1 Housing 21 has a legitimate business purpose for using CCTV on our courts and offices:

- to prevent crime and protect buildings and assets from damage,

disruption, vandalism, and other crime.

- for the personal safety of employees, residents, visitors, and other members of the public and to act as a deterrent against crime.
- to support internal investigations and law enforcement in the prevention, detection, and prosecution of crime, the apprehension of offenders and the prevention and detection of safeguarding incidents.
- to assist in day-to-day management, including ensuring the health and safety of employees, residents, and other individuals in and around Housing 21 premises.
- to assist in the effective resolution of disputes which may arise during disciplinary or grievance proceedings.
- to assist in the defence of any civil litigation, including employment tribunal proceedings; and
- to assist our Insurers or Solicitors to properly consider issues of liability and indemnity.

3.0 Monitoring

3.1 CCTV monitors the exterior and interior of the buildings, communal areas and both the main entrances and secondary exits of courts and the communal areas of offices and can monitor, depending on the identified purpose for which the monitoring is taking place for 24 hours a day. This data is continuously recorded or where applicable, during working hours only.

3.2 Camera locations are chosen to minimise viewing of spaces not relevant to the legitimate purpose of the monitoring. As far as practically possible, CCTV cameras will not focus on private homes, gardens, or other areas of private property.

3.3 Where deemed necessary, surveillance systems will be used to record sound but only where we can clearly justify its use with robust supporting evidence.

3.4 Images are monitored by authorised personnel, the Scheme Manager and/or their Deputy, 'buddy' Scheme Manager only in the instance of suspected wrongdoing, for appropriate time periods in line with identified purpose(s).

3.5 Employees using surveillance systems will be given appropriate training to ensure they understand and observe the legal requirements related to the processing of relevant data.

4.0 CCTV Operation

4.1 Where CCTV cameras are placed in the workplace, we will ensure that signs are displayed at the entrance of the surveillance area to alert individuals that their image may be recorded. Such signs will contain details of the organisation operating the system, the purpose for using the surveillance system and who to contact for further information, where these things are not obvious to those being monitored.

4.2 Live feeds from CCTV cameras will only be monitored where this is reasonably necessary, for example to protect health and safety, or to monitor suspected fraudulent and/or criminal activity.

4.3 We will ensure that live feeds from cameras and recorded images are only viewed by approved employees whose role requires them to have access to such data. This may include HR employees, Legal Counsel and the Data Protection Officer, involved with disciplinary or grievance matters or information rights requests, including third party disclosures (such as law enforcement). Recorded images will only be viewed in designated, secure offices.

5.0 Use of CCTV Footage

5.1 To ensure that the rights of individuals recorded by the CCTV system are

protected, we will ensure that data gathered from CCTV cameras is stored in a way that maintains its integrity and security. This may include encrypting the data, where it is possible to do so.

5.2 Given the large amount of data generated by surveillance systems, we will store video footage using local data repositories in each Court and where necessary, at Tricorn House, which maintains the security of our information, in accordance with industry standards. Where there is a requirement to engage data processors, we will ensure reasonable contractual safeguards are in place to protect the security and integrity of the data.

6.0 Retention and Deletion of CCTV Footage

6.1 Data recorded by CCTV systems will be stored digitally using local data repository systems. Data from CCTV cameras will not be retained indefinitely but will be permanently deleted once there is no reason to retain the recorded information. Exactly how long images will be retained for will vary according to the purpose for which they are being recorded. For example, where images are being recorded for crime prevention purposes, data will be kept long enough only for incidents to come to light, although, in most cases, it is recognised that this is usually within 24/48 hours of an ASB, criminal or accident related incident occurring. In all other cases, recorded images will be kept for no longer than 90 days. Each court and office will maintain a comprehensive log of when data is deleted.

6.2 At the end of their useful life, e.g. at the conclusion of an investigation (and in line with our data retention schedule) all images stored in whatever format will be erased permanently and securely. Any physical matter such as tapes or discs will be disposed of as confidential waste. Any still photographs and hard copy prints will be disposed of as confidential waste. IT will be consulted for any electronic equipment disposal.

7.0 Use of Additional Surveillance Systems

7.1 Prior to introducing any new surveillance system, including placing a new CCTV camera in any workplace location, employees will carefully consider if they are appropriate by carrying out a Data Privacy Impact Assessment (DPIA).

7.2 A DPIA is intended to assist in deciding whether new surveillance cameras are necessary and proportionate in the circumstances and whether they should be used at all or whether any limitations should be placed on their use.

7.3 A DPIA will consider the nature of the problem that employees are seeking to address at that time and whether the surveillance camera is likely to be an effective solution, or whether a better solution exists. Employees will consider the effect a surveillance camera will have on individuals and therefore whether its use is a proportionate response to the problem identified.

7.4 Surveillance cameras will not be placed in areas where there is an expectation of privacy (for example, in changing rooms) unless, in exceptional circumstances, it is judged by Housing 21 to be necessary to deal with very serious concerns. These will be managed on a case by case basis and require authorisation from the Deputy Chief Executive or in their absence an Executive Director.

8.0 Covert Monitoring

8.1 Housing 21 will never engage in covert monitoring or surveillance (that is, where individuals are unaware that the monitoring or surveillance is taking place) unless, in highly exceptional circumstances, there are reasonable grounds to suspect that criminal activity or extremely serious malpractice is taking place and, after suitable consideration, having

undertaken a DPIA, we reasonably believe there is no less intrusive way to tackle the issue.

8.2 In the rare event that covert monitoring is justified, it will only be carried out with the express authorisation of the Deputy Chief Executive or where they are not available, an Executive Director. The decision to carry out covert monitoring will be fully documented and will set out how the decision to use covert means was reached and by whom. The risk of intrusion on innocent workers will always be a primary consideration in reaching any such decision.

8.3 Only limited restricted authorised individuals will be involved in covert monitoring. This requires sign off from an Executive Director, the Deputy Chief Executive, (currently the SIRO) and liaison with the Data Protection Officer (DPO). Please refer to the CCTV Procedure for full details.

8.4 Covert monitoring will only be carried out for a limited and reasonable period consistent with the objectives of making the recording and will only relate to the specific suspected illegal or unauthorised activity.

9.0 Review of CCTV Use

9.1 Housing 21 will ensure that the ongoing use of existing CCTV cameras in the workplace is reviewed periodically to ensure that their use remains necessary and appropriate, and that any surveillance system is continuing to address the needs that justified its introduction.

10.0 Requests for Disclosure

10.1 Housing 21 may share data with other associated companies or organisations, for example shared services partners and data sharing agreement partners where we consider that this is reasonably necessary for any of the legitimate purposes, outlined in the DPA18 and the

UKGDPR.

10.2 Images from our CCTV cameras will not be disclosed to any other third party, without express permission being given by the organisations Data Protection Officer (DPO). Data will not normally be released unless satisfactory evidence that it is required for legal proceedings or under a court order has been produced.

10.3 In other appropriate circumstances, we may allow law enforcement agencies to view or remove CCTV footage where this is required in the detection or prosecution of crime.

10.4 We will maintain a record of all disclosures of CCTV footage.

10.5 Images from CCTV will never be posted online or disclosed to the media.

11.0 Data Subject Access Requests

11.1 Individuals may make a request for disclosure of their personal information, and this may include CCTV images. This can be done by submitting a data subject access request. Please refer to the Data Subject Access Request (DSAR) Procedure and Form for more detail.

11.2 For Housing 21 to locate relevant footage, any requests for copies of recorded CCTV images must include the date and time of the recording, the location where the footage was captured and, if necessary, information identifying the individual.

11.3 Housing 21 reserve the right to obscure images of third parties when disclosing CCTV data as part of a data subject access request, where we consider it necessary to do so.

12.0 Complaints

12.1 If an employee or resident has questions about this policy or any concerns about our use of CCTV, then they should speak to their manager, scheme manager, the relevant Executive Director and/or the Data Protection Officer (DPO).

12.2 Where this is not appropriate or matters cannot be resolved informally, employees should use our formal grievance procedure and resident can submit a concern through the approved Complaints and Compliments process.

13.0 Requests to Prevent Processing

13.1 Housing 21 recognise that, in rare circumstances, individuals may have a legal right to prevent processing likely to cause substantial and unwarranted damage, or to prevent automated decision making. For further information regarding this, please contact the Data Protection Officer (DPO).

14.0 Data Protection Provisions

14.1 Privacy Notice – Transparency of Data Protection
Being transparent and providing accessible information to individuals about how we use their personal data is important to Housing 21. The following details how we collect data and process data:

What information is being collected	CCTV images of individuals
Who is collecting it	Housing 21
How is it collected	By CCTV cameras and other surveillance equipment
Why is it being collected	For the legitimate business purposes as identified, from time to time, within the business, such

	as the prevention and detection of crime.
How will it be used	It will be used as evidence. The evidence will be used to in court, if necessary, to prove someone was in a certain place or that they committed an offence. It will also be used to improve court and building safety and prevent crime, by putting people off committing crimes like robbery if they know their actions are being recorded.
Who will it be shared with	Third parties such as law enforcement agencies and partners with whom we have data sharing agreements and shared services.
Identity and contact details of any data controllers	Housing 21, Tricorn House, 51-53 Hagley Road, Birmingham B16 8TP. dataprotection@housing21.org.uk
Details of transfers to third country and safeguards	None.
Retention period	Information will be kept only as is strictly necessary to meet our purposes for recording it but for no longer than 90 days.

15.0 Conditions for Processing

15.1 All employees who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing are available to employees and all data subjects in the form of Housing 21's privacy notice and CCTV Privacy Notices displayed where CCTV monitoring is being undertaken.

16.0 Justification for Processing Personal Data

16.1 Housing 21 will process personal data in compliance with all six data protection principles. We will document the additional justification for the processing of sensitive data and will ensure any biometric and genetic data is considered sensitive.

17.0 Grounds for Processing

17.1 The data we collect is subject to implied or active consent by the data subject, as appropriate. In cases of active consent this can be revoked at any time. Where it is in the legitimate interests of the business or where we must satisfy our legal obligations, we shall collect data.

18.0 Data Profiling and Automated Decision Making

18.1 We will only carry out solely automated decision-making, which includes profiling, with legal or similarly significant effects if the decision is:

- necessary for entering or performance of a contract between Housing 21 and the data subject.
- authorised by law (for example, for the purposes of fraud or tax evasion)
- based on the data subject's explicit consent; or
- the processing is necessary for reasons of substantial public interest.

18.2 Housing 21 do not routinely engage in automated decision-making.

19.0 Data portability

19.1 Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within 30 calendar days, provided there is no undue burden, and it does not compromise the privacy of other individuals. A data subject may

also request that their data is transferred directly to another system. This must be done for free. Where a request of this nature is submitted, always seek guidance form the Data Protection Officer.

20.0 Right to be forgotten

20.1 A data subject may request that any information held on them is deleted or removed and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

21.0 Privacy by Design and Default

21.1 Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The DPO will be responsible for ensuring relevant Data Protection Impact Assessments are in place.

21.2 When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

22.0 International Data Transfers

22.1 No data may be transferred outside of the EEA without first discussing it with the DPO and the Cyber Security Manager. Specific consent from the data subject must be obtained prior to transferring their data outside the EEA unless exemptions apply, such as it is in the legitimate interests of the business of Housing 21 for the transfer to occur.

23.0 Data Audit and Register

23.1 Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

24.0 Reporting Breaches

24.1 All employees have an obligation to report actual or potential data protection breaches. This enables us to:

- Investigate the failure and take remedial steps if necessary.
- Maintain a register of compliance failures.
- Notify the Information Commissioners Office (ICO) of any compliance failures that are material either or as part of a pattern of failures.

25.0 Monitoring

25.1 All employees must observe this policy. The DPO has overall responsibility for this policy. The DPO will monitor processes relating to the policy regularly to ensure it is being adhered to.

26.0 Failing to Comply

26.1 We take compliance with this policy very seriously. Failure to comply puts both you, your colleagues, our residents, and the organisation at risk. Failure to comply with any requirement of this policy may lead to disciplinary action under our procedures which may result in dismissal. If you have any questions or concerns about anything in this policy, do not hesitate to contact the Data Protection Officer, at dataprotection@housing21.org.uk.

27.0 Related Polices & Guidance

- Data Protection Policy & Procedure
- Privacy Notice
- IT Acceptable Use Policy

- Subject Access Request Procedure
- Information Governance & Security Policy and Procedures
- Equality, Diversity and Inclusion Policy
- CCTV Surveillance Procedure
- Domestic CCTV Systems – Including Guidance for Residents
- Service Charge Policy
- Choice and Consensus Policy

Related Legislation

- Data Protection Act 2018
- UK General Data Protection Regulation