POLICY DOCUMENT

Group Member:	Progress Housing Group
Service Area:	Data Protection
Document Ref No:	GRPOLDP01
Subject Title:	CCTV Policy
Version:	5
Effective Date:	01/06/2010
Last Reviewed:	24/02/2021
Next Review Date:	01/02/2024

Document Owner:	Head of Business Assurance
Date of Board Approval:	24/02/2021

1. INTRODUCTION

1.1 This policy defines how Progress Housing Group ("the Group") and its subsidiaries will implement and manage Closed Circuit Television systems ("CCTV").

1.2 The policy is to ensure compliance with Data Protection Legislation (including the Data Protection Act 2018 and General Data Protection Regulation as amended by statutory instruments), Protection of Freedoms Act 2012, and the linked Information Commissioner's Office ("ICO")Code of Practice for Surveillance Cameras and Personal Information and the Home Office Surveillance Camera Code of Practice.

1.3 By ensuring compliance with the above legislation and guidance, we ensure the privacy and rights of the public are upheld, whilst also enabling use of CCTV for its required purpose(s).

2. SCOPE OF THE POLICY

2.1 This policy applies to all staff of the Group who manage the implementation of CCTV systems, oversee the operational maintenance and maintenance contracts for CCTV and anyone operating CCTV systems either on an active day-by-day basis or purely for the purposes of reviewing and retrieving recorded activity, on those CCTV systems

2.2 This policy applies to external suppliers who supply, maintain, operate and remove CCTV systems on behalf of the Group acting as a 'Data Processor'.

2.3 It will cover all the Group sites, where CCTV is already implemented and sites where CCTV is proposed for implementation.

2.4 It will not cover sites where CCTV is controlled (installed, managed and/or operated) by another company or organisation designated as 'Data Controller' for that system, unless they are contracted as a 'Data Processor' by the Group.

2.5 This policy will cover the Groups use of Overt CCTV

2.6 The Group does not use General Covert CCTV

2.7 The Group does not use unmanned aerial systems, automatic number plate recognition, body worn video, biometric characteristic recognition or facial recognition

2.8 This policy will not cover Directed Covert CCTV implemented by the Community Safety Team or other third parties on the Groups behalf. This is covered by the Community Safety Covert Surveillance Policy.

2.9 This policy will not cover personal CCTV in the individual properties we let, held and managed for the purposes of our tenants own personal use. Any such footage disclosed to the Group by the 'controller' (the controller being the owner/operator of the system), from that CCTV System, would fall under the Data Protection Policy, and depending on the circumstances of the disclosure, the Community Safety Team's Covert Surveillance Policy.

3. RESPONSIBILITY

3.1 The Board of Directors have overall responsibility to ensure compliance across the Group with this policy and legislation relating to CCTV

3.2 The Legal Director has operational responsibility to ensure the recording of all CCTV Assets & Liabilities across the Group.

3.3 The Data Protection Officer ("DPO")is responsible for the implementation, maintenance and dissemination of this policy

3.4 Managers and operational staff are responsible for ensuring they and their colleagues comply with this policy in the day-to-day execution of their roles, ensuring the requirements of this policy are explained and complied with by suppliers and contractors

3.5 Suppliers and contractors must also comply with the current Data Protection legislation where they are implementing, operating or managing CCTV systems on behalf of the Group. The terms of this policy, where appropriate, should be translated into the supplier contracts and our requirements, ensuring they're aware of their obligations under the legislation and specifying them as a Data Processor. This must include the ability to evidence their compliance and allow for auditing of their legal compliance.

4. POLICY

4.1 Aims & Objectives

All CCTV systems will comply with the 12 principles of the Surveillance Camera Code of Practise through the following actions:

4.1.1 All CCTV systems will have a documented specific purpose, which is in pursuit of a legitimate aim and necessary to meet an identified pressing need;

4.1.2 All CCTV systems will have an affiliated Data Protection Impact Assessment, which must be put in place before a new system is implemented and will be reviewed annually or in advance of any changes to the CCTV in scope, use, or technology;

4.1.3 All CCTV systems will have signage defining who is operating the CCTV system, including a contact point for access to information and complaints together with the purpose for the CCTV system, this signage must be clearly visible on entry into any space covered by CCTV with additional signage in close proximity to the camera,;

4.1.4 4.1.3 does not apply to specially sanctioned covert surveillance;

4.1.5 All CCTV systems will have a defined manager and operator roles, with those roles and related tasks and responsibilities clearly defined;

4.1.6 There will be a defined procedure attached to each CCTV system, to define how it should be operated and used. The procedure must be communicated to all who need comply with it

4.1.7 There will be over-arching procedures to determine the planning, selection, implementation, operation, maintenance, review and retirement of CCTV systems;

4.1.8 There will be defined procedures regarding Data Disclosure either as set out in ‘Subject Access Request Procedure’ or ‘Third Party Disclosure Procedure’;

4.1.8.1 All instances of data disclosure must be raised with the DPO and a log of the disclosure recorded, in-line with the above procedures;

4.1.9 CCTV images and/or data, including but not limited to recorded video, will not be held on the CCTV system for longer than it is required for the stated purpose, to enable action and/or retrieval in respect to any requests. This is a period no longer than 31 days;

4.1.10 Extracted CCTV images and/or data on removable media, must be held according to the Groups retention schedule and stored securely, to prevent accidental loss or theft and also if required for future references if required for a legal case;

4.1.10.1 A log must be kept of any extracted data stored, accessed and destroyed;

4.1.10.2 Where feasible extracted data should be encrypted to better guarantee security, this is a mandatory requirement for all new CCTV installations and upgrades;

4.1.10.3 Any stored extracted data will be deleted once its stated purpose has been discharged.

4.1.11 CCTV systems equipment (recorders, displays and cameras) are to be kept secure to prevent tampering, damage or destruction of data or illegitimate disclosure of data. This is to ensure the adequacy of the data;

4.1.11.1 Cameras should be placed to ensure they are free of obstructions. Consideration should be given to seasonal elements such as tree growth etc. to ensure ongoing adequacy of the footage;

4.1.11.2 Cameras must not capture the private property of others without their prior written permission. Digital or physical masking must be used where this is physically unfeasible;

4.1.11.3 4.1.11.3 does not apply to boundary walls, fences, or the walls of properties in a communal corridor but specifically applies to any situation where a person could be seen behind such barriers such as through glazing or gaps in fences etc.;

4.1.11.4 Where feasible cameras should not be easily accessible for tampering with and where necessary security measures, such as protective covering put in place;

4.1.11.5 CCTV display screens should not be openly visible to the public;

4.1.11.6 Where CCTV display screens are actively monitored, access and visibility to the screen(s) should be limited and secured as best as possible. Signage should inform Data Subjects that the CTV is actively monitored;

4.1.12 Only authorised Group staff have access to CCTV systems and all staff should ensure the legitimacy of external support and maintenance staff who are granted access to the CCTV system(s);

4.1.12.1 Where CCTV systems are linked to the internet and made available remotely, appropriate security safeguards must be

put in place to ensure security of the data and prevent illegitimate access and tampering;

4.1.12.2 Appropriate inductions and training will be provided to all authorised Group staff who deal with the CCTV systems. This includes communication of relevant policies and procedures and ensuring that officers who review CCTV images hold the relevant qualifications/licences required to do so.

4.1.13 CCTV systems must be regularly maintained as laid out in their maintenance and service contracts;

4.1.13.1 Recording devices should have regular software and firmware updates applied within a reasonable time of them being made available by the manufacturer;

4.1.13.2 Cameras should be maintained, cleaned and kept in good working order;

4.1.14 Monthly reviews should be made to ensure the effectiveness, validity and quality of the systems, ensuring all cameras are operational and recordings and their related metadata are valid (e.g. date and time stamps, camera position or name, etc.);

4.1.15 An audit log should be maintained of all actions carried out against the CCTV system, whether maintenance, support tasks or data retrieval;

4.1.16 Annual reviews should ensure the effectiveness of the CCTV System in relation to its initial purpose, aim and need. Where these aims are no longer met, the CCTV system should be retired, or made fit for purpose;

4.1.17 Any unauthorised access or loss of data, either on the device or on removable media (CD, DVD, USB Pen etc.) must be reported immediately to the Data Protection Officer in conjunction with the Data Breach Handling Process.

4.1.18 Any complaint received in connection with a CCTV system will be dealt with pursuant to the Complaints Procedure.

4.2 Definitions

1.1.1 **Overt CCTV**: Overt surveillance is carried out with the full knowledge of staff, residents and the public, whose images are captured using the system. The cameras are on open display and there are signs around the building advertising

their use. This is a common method of deterring vandalism theft or anti-social behaviour. The images may be retrieved should an incident occur, as an aid to the identification of the perpetrator and subsequent action. On-going observation of the CCTV images may be required, to ensure ongoing safety of individuals where there is a legitimate purpose to do so.

1.1.2 **Covert CCTV** (or General Covert CCTV): Covert surveillance is when the cameras are not advertised and are hidden from view. Images are captured without the knowledge of residents or the public and are usually monitored as an ongoing process. Progress Housing group does not use this method of CCTV.

1.1.3 **Directed Covert CCTV**: Directed covert surveillance, is when a camera is secretly put in place and hidden from view. There are no signs displayed to inform the residents or local people that cameras are in operation, so as not to prejudice the purpose of the cameras installation. It is usually carried out in response to a serious or ongoing problem of criminal or anti-social behaviour (ASB) activity. In this case, cameras are installed for a fixed period of time, as an attempt to gather evidence. The images will be monitored at the end of the fixed period, to see if evidence of the ASB or criminal activity has been captured. This type of CCTV is covered by the Community Safety Covert Surveillance Policy. The Data Protection Officer (DPO) must be informed in advance of any form of covert surveillance unless the DPO is the subject of that surveillance or there are strong reasons for believing that informing the DPO would jeopardise the investigation or the DPO is uncontactable within the necessary time. Where the DPO is not informed, the Head of Business Assurance and the Group Chief Executive will be informed in place of the DPO.

1.1.4 **Data Controller** means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

1.1.5 **Data Processor** in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

4.3 References

4.3.1 Data Protection Legislation including the Data Protection Act 2018 and General Data Protection Regulation (both as amended by statutory instruments) – CCTV usage must be compliant with these laws

4.3.1.1 The ICO's CCTV Code of Practise, expands on the DPA applying it specifically to CCTV & surveillance systems and forms the basis for this policy

4.3.2 Human Rights Act 1998 – the Data Protection Act is based up on human right to privacy, with certain exceptions relating to criminal activity

4.3.3 Protection of Freedoms Act 2012 (POFA)

4.3.4 Home office Surveillance Camera Code of Practise, derived from the POFA

4.4 Data Protection

This policy is written as a companion to the Data Protection Policy, defining specific applicable terms for CCTV installations. All terms of the Data Protection Policy and related legislation apply to all CCTV installations, and are based upon data protection legislation and related guidance, including the Principles, roles and exemptions.

5. IMPLEMENTATION

5.1 Training

Training will be provided to all managers and operators. This will cover operation of the system so that footage can be reviewed and retrieved.

Written procedures and work instructions should support this training for future reference.

5.2 Procedure references

5.2.1 Subject Access Request Procedure

5.2.2 Data Disclosure Procedure

5.2.3 CCTV Implementation, Operation & Removal Procedure

5.2.4 Data Retention and Disposal Schedule & Procedure

5.2.5 Complaints Procedure.

5.3 Linked documents

5.3.1 Data Protection Policy

5.3.2 Information Security Policy

5.3.3 Community Safety Covert surveillance policy

6. CONSULTATION

6.1 External legal consultation has been sought to ensure this policy is appropriate and legally compliant

7. REVIEW

7.1 This policy should be reviewed every 3 years, or in line with changes in legislation

7.2 Related Procedures may be reviewed more often to ensure efficiencies

8. EQUALITY IMPACT ASSESSMENT

8.1 The equality impact assessment for this policy has been reviewed and updated, but continues to be assessed as a low impact on those with protected characteristics.