Arun District Council's CCTV Policy

This policy outlines how the District Council will use CCTV surveillance camera systems where it is the data controller, detailing safeguards to ensure lawful processing of the data concerned. Such systems fall into two principal categories. Firstly, those installed across its estate (General Fund and Housing Revenue Account). Secondly, the CCTV surveillance camera systems it may require as regulator be installed in privately owned regulated places such as taxis.

Note: This policy takes into account the Surveillance Camera Commissioner's Surveillance Camera Code of Practice, EU General Data Protection Regulation which took effect on 25 May 2018 and the Home Office Surveillance Camera Code of Practice (November 2021).

1. POLICY STATEMENT – GUIDING PRINCIPLES

1.1 The Council believe that CCTV surveillance camera systems have a legitimate role to play in helping to maintain a safe and secure environment for all our staff and visitors including persons coming to the premises to visit persons sharing our premises. However, the Council recognise that this may raise concerns about the effect on individuals and their privacy. This policy is intended to address such concerns. Images recorded by CCTV surveillance camera systems are personal data which must be processed in accordance with data protection laws. The Council is committed to complying with our legal obligations and ensuring that the legal rights of those captured on CCTV images, relating to their personal data, are recognised and respected.

1.2 This policy is intended to assist staff in complying with their own legal obligations when working with personal data. In certain circumstances, misuse of information generated by CCTV or other surveillance camera systems could constitute a criminal offence.

1.3 This policy does not relate to body worn cameras, vehicle-mounted cameras, camera system used for streaming and recording public meetings of Full Council and Council Committees, cameras in the public domain operated by Sussex Police, covert surveillance by the Council as a prosecuting authority under the Regulation of Investigatory Powers Act or ANPR vehicle number plate monitoring or similar systems. Where these activities are carried out by the Council they are the subject of separate policies or procedures. This policy does not relate to nor seek to prohibit the use of "dummy" CCTV cameras, as these are not surveillance camera systems.

2. DEFINITIONS

2.1 For the purposes of this policy, the following terms have the following meanings:

- **CCTV;** means dedicated fixed and domed cameras designed to capture and record

images of individuals and property.

- **Council;** means the Arun District Council.

- **Data**: is information which is stored electronically, or in certain paper-based filing systems. In respect of CCTV, this generally means video images. It may also include static pictures such as printed screen shots.

- **Data subjects**: means all living individuals about whom the Council hold personal information as a result of the operation of our CCTV (or other surveillance camera systems). This includes employees, councillors, contractors or members of the public visiting Council premises.

- **Personal data**: means data relating to a living individual who can be identified from that data (or other data in our possession). This will include video images of identifiable individuals.

- **Data controllers**: are the people who, or organisations which, determine the manner in which any personal data is processed. They are responsible for establishing practices and policies to ensure compliance with the law. The Council is the data controller of all personal data used in our business for our own commercial purposes and oversight of this role will be carried out by the Council's Data Protection Officer (the Group Head of Law & Governance). The Council is the data controller where it may choose to mandate use of CCTV surveillance camera systems in regulated places.

- **Data users**: are those of our employees whose work involves processing personal data. This will include those whose duties are to operate CCTV cameras and other surveillance camera systems to record, monitor, store, retrieve and delete images. Data users must protect the data they handle in accordance with this policy.

- **Data processors**: are any person or organisation that is not a data user (or other employee of a data controller) that processes data on our behalf and in accordance with our instructions (for example, a supplier which handles data on our behalf).

- **DPO**: means the Data Protection Officer (the Group Head of Law & Governance) or in their absence the person deputising for the Data Protection Officer.

- **Processing**: is any activity which involves the use of data. It includes obtaining, recording or holding data, or carrying out any operation on the data including organising, amending, retrieving, using, disclosing or destroying it. Processing also includes transferring personal data to third parties.

- **SRO**: Senior Responsible Officer – Group Head of Law & Governance

- **SPOC**: Single Point of Contact with the Biometrics and Camera Surveillance

Commissioner - Group Head of Technical Services

- **Surveillance camera 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 automatic number plate recognition (ANPR), body worn cameras, unmanned aerial systems and any other systems that capture information of identifiable individuals or information relating to identifiable individuals.

- **We**: Means Arun District Council

3. ABOUT THIS POLICY

3.1 We currently use CCTV cameras to view and record individuals on and around our premises. This policy outlines why we use CCTV, how we will use CCTV and how we will process data recorded by CCTV cameras to ensure we are compliant with data protection law and best practice. This policy also explains how to make a subject access request in respect of personal data created by CCTV.

3.2 We recognise that information that we hold about individuals is subject to data protection legislation. The images of individuals recorded by CCTV cameras are personal data and therefore subject to the legislation. We are committed to complying with all our legal obligations and seek to comply with best practice suggestions from the Information Commissioner's Office (ICO).

3.3 This policy covers all employees, consultants, contractors, volunteers, work experience students, casual workers, zero hours workers and agency workers and may also be relevant to members of the public visiting our premises and residents of Council housing. This policy is also applicable to external organisations, Council tenants or members of the public wishing to access CCTV images held by the Council.

3.4 This policy has been adopted following consultation with Unison via the Formal Staff Unison Consultation Panel.

3.5 This policy is non-contractual but as a policy of the Council, the requirement to observe the policy forms part of the terms and conditions of any employment or other contract. We may amend this policy at any time following consultation with Unison. The policy will be regularly reviewed by the DPO to ensure that it meets legal requirements, relevant guidance published by the ICO and industry standards.

3.6 A breach of this policy may, in appropriate circumstances, be treated as a disciplinary matter. Following investigation, a breach of this policy or the relevant data protection legislation may be regarded as misconduct or gross misconduct leading to disciplinary action, up to and including dismissal as covered by the Staff & Manager's Handbook and related procedures.

4. PERSONNEL RESPONSIBLE

4.1 The DPO 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 Group Heads and Directors. Day-to-day operational responsibility for CCTV cameras and the storage of data recorded is the responsibility of the Repairs and Contracts Manager on our Council Housing sites and the Property, Estates & Facilities Manager on our other sites.

4.2 Responsibility for keeping this policy up to date has been delegated to the DPO

5. REASONS FOR THE USE OF CCTV

5.1 We currently use CCTV around our estate as outlined below. We believe that such use is necessary for legitimate business purposes, including:

- **a)** prevent crime and protect buildings and assets from damage, disruption, vandalism and other crime;
- **b)** for the personal safety of staff, visitors and other members of the public and to act as a deterrent against crime;
- **c)** to support law enforcement bodies in the prevention, detection and prosecution of crime;
- **d)** to assist in day-to-day management, including ensuring the health and safety of staff and others;
- **e)** to assist in the effective resolution of disputes which arise in the course of disciplinary or grievance proceedings, and;
- **f)** to assist in the defence of any civil litigation, including employment tribunal proceedings

This list is not exhaustive and other purposes may be or become relevant but will only be applied with the express written determination of the DPO.

5.2 As a public body the Council may also need to process CCTV footage for the necessary performance of a task carried out in the public interest or in the exercise of official authority vested in the Council.

6. MONITORING

6.1 CCTV monitors Council owned buildings/land 24 hours a day and this data is continuously recorded.

6.2 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. Location and angles will be considered and we will attempt to ensure that annual or other changes (such as growth of plants and trees) are

reasonably taken into account in this consideration.

6.3 The Council's CCTV surveillance camera systems will not be used to record sound. The exception to this is the CCTV systems that the Council may mandate be installed and operated in privately owned regulated locations such as taxis and private hire vehicles. In this scenario, although the hardware is owned by the vehicle owner, the Council is the data controller. The audio recordings will be capable of being turned on/off and conditions attached to licences to control operation, data retention and sharing arrangements.

6.4 Facial recognition software will not be used.

6.5 Images may be monitored by authorised personnel 24 hours a day every day of the year, subject to principles in paragraph 7.2.

6.6 Staff using CCTV surveillance camera systems will be given appropriate training to ensure they understand and observe the legal requirements related to the processing of relevant data.

6.7 The DPO will authorise persons for the purposes of 6.5 above and shall be responsible for selecting and completion of the training referred to in 6.6 above.

7. HOW WE WILL OPERATE ANY CCTV

7.1 Where CCTV cameras are placed on our estate, we will ensure that signs are displayed at the entrance of the surveillance zone 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. The Repairs and Contracts Manager on our Council Housing sites and the Property, Estates & Facilities Manager on our other sites will be responsible for reviewing the location of signage annually.

7.2 Live feeds from CCTV cameras will only be monitored where this is reasonably necessary, for example to protect health and safety, or checking systems are working correctly.

7.3 We will ensure that live feeds from cameras and recorded images are only viewed by members of staff whose role requires them to have access to such data and are authorised by the DPO, or their deputy. Recorded images will only be viewed in designated, secure offices by officers authorised by the DPO, or their deputy. Recorded images may be viewed Human Resources staff and investigating/hearing managers' involved with disciplinary or grievance matters.

8. USE OF DATA GATHERED BY CCTV

8.1 In order 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.

8.2 Given the large amount of data generated by surveillance camera systems, we may store video footage using a cloud computing system. We will take all reasonable steps to ensure that any cloud service provider maintains the security of our information, in accordance with industry standards.

8.3 We may engage data processors to process data on our behalf. We will ensure reasonable contractual safeguards are in place to protect the security and integrity of the data.

9. RETENTION AND ERASURE OF DATA GATHERED BY CCTV

9.1 Data recorded by the CCTV system will be stored and this may include storage digitally using a cloud computing system. 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. Data downloaded for use within an investigation may be stored for a longer period to facilitate the investigation, and potential appeal. In all other cases, recorded images will be kept for no longer than 30 [thirty] days. The Repairs and Contracts Manager on our Council Housing sites and the Property, Estates & Facilities Manager will maintain a comprehensive log of when data is deleted which must be made available to the DPO on request.

9.2 At the end of their useful life, all images stored in whatever format will be erased permanently and securely. Any physical matter such as discs will be disposed of as confidential waste. Any still photographs and hard copy prints will be disposed of as confidential waste.

10. USE OF ADDITIONAL SURVEILLANCE CAMERA SYSTEMS

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

10.2 A DPIA is intended to assist us 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.

10.3 Any DPIA will consider the nature of the problem that we 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. In particular, we will consider the effect a surveillance camera will have on individuals and therefore whether its use is a proportionate response to the problem identified.

10.4 No surveillance cameras will be placed in areas where there is an expectation of privacy (specifically this means in changing rooms, rest rooms and kitchen areas) unless, in very exceptional circumstances, it is judged by the DPO to be necessary to deal with very serious concerns. Such decisions will be recorded on the DPO register of decisions. An example of exceptional circumstances might be if there were allegations of criminal damage in a kitchen or rest room area. In such cases use of surveillance cameras will be overt and signage will be used.

10.5 Leases of Council owned land/property will from the date of adoption of this policy, include a clause requiring landlord approval prior to installation of any CCTV camera surveillance camera systems by tenants. Landlord consent will only be issued where a written undertaking is provided by the tenant that they will follow ICO guidance and in the case of the Council's housing tenants, that nowhere outside the leased property is within the surveillance zone unless they do so. A record of this undertaking will be retained on the corresponding entry in the asset management system.

11. COVERT MONITORING

11.1 We will not 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, we reasonably believe there is no less intrusive way to tackle the issue.

11.2 In the unlikely event that covert monitoring is considered to be justified, it will only be carried out with the express authorisation of the Chief Executive or a 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 people not involved in the suspected serious malpractice or criminal activity will always be a primary consideration in reaching any such decision.

11.3 Only a limited number of people will be involved in any covert monitoring.

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

11.5 Covert Directed Surveillance (that is for a specific investigation or a specific operation, likely to result in private information about a person being obtained) is subject to the Council's Corporate Policy And Procedures Document On The Regulation Of Investigatory Powers Act 2000 (RIPA).

12. ONGOING REVIEW OF CCTV USE

12.1 We will ensure that the ongoing use of existing CCTV cameras on our estate is reviewed periodically to ensure that their use remains necessary and appropriate, and that any surveillance camera system is continuing to address the needs that justified its introduction, including consideration of the adequacy of image quality.

12.2 The review will be conducted by the SRO and SPOC.

13. REQUESTS FOR DISCLOSURE

13.1 We may share data with other organisations, for example shared services partners delivering services from our premises or other persons occupying part of the Council premises where we consider that this is reasonably necessary for any of the legitimate purposes set out above in Paragraphs 5.1 or 5.2.

13.2 No images from our CCTV cameras will be disclosed to any other third party, without express permission being given by the DPO. Data will not normally be released unless satisfactory evidence that it is required for legal proceedings or with the terms of a court order that has been produced.

13.3 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. In such circumstances a documented request for release must be received prior to release.

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

13.5 No images from CCTV will ever be used for commercial purposes or entertainment, but may be posted online or disclosed to the media by law enforcement agencies for the purposes of identifying suspects.

14. SUBJECT ACCESS REQUESTS

14.1 Data subjects may make a request for disclosure of their personal information and this may include CCTV images (**data subject access request**). A data subject access request is subject to the statutory conditions from time to time in place and should be made in writing, in accordance with our subject access procedure.

14.2 In order for us 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.

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

15. COMPLAINTS

15.1 If any member of staff has questions about this policy or any concerns about our use of CCTV, then they should speak to their manager or the Group Head of Law & Governance.

15.2 Where this is not appropriate or matters cannot be resolved informally, employees can use the Council's formal Grievance Procedure.

15.3 If any member of the public has a question or concern about the use of our CCTV policy, this can be made using our Corporate Complaints Process.

16. REQUESTS TO PREVENT PROCESSING

16.1 We recognise that, in rare circumstances, individuals may have a legal right to object to processing and in certain circumstances to prevent automated decision making (see Articles 21 and 22 of the General Data Protection Regulation). For further information regarding this, please contact the DPO.