Surveillance Camera Systems Policy and Code of Practice

At a glance …

- The use of overt surveillance cameras such as town centre CCTV systems can be particularly intrusive to the privacy of individuals. Their use must be necessary, proportionate and adequate for the specified purpose they are there to address.

- The Council will have regard to relevant Codes of Practice and this policy document in its use of surveillance cameras.

- There must be a clear and lawful justification for the use of surveillance cameras. Other options for achieving the same ends must be considered.

- A surveillance camera system specific Data Protection Impact Assessment (DPIA) must be completed for all new systems before they become operational. DPIAs will also be completed for existing systems.

- There must be appropriate information and signage and privacy information to advise of the use of overt surveillance cameras.

- The Council's Regulation of Investigatory Powers Act 2000 Policy and guidance document applies to the use of covert surveillance cameras.

- All suppliers of surveillance cameras systems will have a contract with the Council that has appropriate data protection clauses.

- All surveillance camera systems will have a designated owner responsible for compliance with this procedure. The owner may appoint system operators.

- Request for surveillance camera images by people asking for their own data, or by third parties (i.e. a Subject Access Request) under the Data Protection Act 2018 or as part of Freedom of Information request should only be dealt with in accordance with this policy.

- The Council's Director of Organisational Development and Democratic Services is the Senior Responsible Officer for overt surveillance camera systems and will be the Council's point of contact with the Surveillance Camera Commissioner.

- The Community Protection Manager is the single point of contact (SPOC) in respect of all operational issues and questions in relation to surveillance camera systems.

- A corporate register of all surveillance camera systems will be maintained by the Senior Responsible Officer for overt surveillance camera systems.

1.0 Introduction

1.1 Gedling Borough Council (the Council) operates surveillance cameras including Closed Circuit Television (CCTV) cameras for a number of purposes. This includes the security of Council premises and car parks; security of personnel (bodycams), the monitoring of accidents and employee safety (for example cameras on refuse vehicles).

1.2 The Council recognises that the use of surveillance cameras can be intrusive and is committed to ensuring that the relevant codes of practice inform its use of surveillance cameras.

1.3 The role of the Surveillance Camera Commissioner (SCC) is to encourage compliance with the Surveillance Camera Code of Practice. The Protection of Freedoms Act 2012 requires all local authorities operating surveillance cameras to pay due regard to this Code of Practice.

1.4 The role of the Information Commissioner's Office (ICO) is to oversee implementation of data protection laws including the Data Protection Act 2018. The ICO CCTV Code of Practice provides guidance for use of surveillance systems and is designed to explain the legal requirements operators of surveillance cameras are required to meet to comply with data protection law.

1.5 In setting this policy the Council has had regard to the following legislation:

- The Data Protection Act (DPA) 2018;
- The EU General Data Protection Regulation (GDPR) and laws implementing or supplementing the GDPR;
- The Human Rights Act 1998;
- The Regulation of Investigatory Powers Act 2000;
- The Freedom of Information Act (FoIA) 2000;
- The Protection of Freedoms Act (PoFA) 2012.

2.0 Scope and Definitions

2.1 This policy forms part of the suite of documents that comprise the Council's Information Governance Framework and should be read in conjunction with these other documents:

- Data Protection Policy and Appropriate Policy Document
- Information Security Policy
- Records Retention and Disposal Policy
- Detailed Employee Guidance on Access to Information
- Information Asset Registers
- Any Data Processing or Information Sharing Agreements
- Any system specific Data Protection Impact Assessments

2.2 This policy applies to all overt surveillance cameras operated by the Council, regardless of whether mobile or fixed or the means by which they are put in place (ie on bodies; in cars or other vehicles; on or in buildings; on drones etc.)

2.3 This policy does not apply to covert surveillance. There are strict rules on covert surveillance. Please refer to the Council's Regulation of Investigatory Powers Act 2000 Policy and guidance and seek advice from the Council's Legal Services team if covert surveillance is being considered.

2.4 A surveillance camera system is defined as the cameras and all the related hardware and software for transmitting, processing and storing the data which is captured.

2.5 Information in this procedure is used as a collective term primarily to describe personal data collected through the use of surveillance camera systems.

2.6 Recorded material is defined as a DVD, CD or still image (including audio and electronic files) or digital storage device (hard drive/usb) and contains data from the CCTV systems.

2.7 A data controller is defined as an organisation that determines how and why personal data is collected and used. The Council is a data controller.

2.8 A data processor acts under the instruction of a data controller and may collect, store and use personal data on the controller's behalf. Surveillance camera system suppliers are data processors.

2.9 A data subject is defined as an identified or identifiable individual to whom personal data relates.

3.0 Purpose of the system

3.1 The Council will ensure that its surveillance camera systems will only be used for legitimate purposes and always in accordance with this policy. The following are relevant lawful purposes:

- To prevent crime and protect buildings and assets from damage, disruption, vandalism and other crime;
- For the personal safety of staff, visitors and other members of the public and to act as a deterrent against crime;
- To support law enforcement bodies in the prevention, detection and prosecution of crime;
- To assist in day-to-day management, including ensuring the health and safety of staff and others;

- To assist in the effective resolution of disputes which arise in the course of customer complaints or internal disciplinary or grievance proceedings;

- To assist in the defence of any civil litigation, including but not limited to insurance claims or employment tribunal proceedings.

3.2 The above list is not exhaustive and other lawful purposes may be considered or become relevant.

3.3 Any data captured by any surveillance camera system may be used for other legitimate purposes where it is reasonable, justified and proportionate to do so with the relevant authorisation in place and where permitted by relevant legislation.

3.4 This policy will be supplemented by operational/procedural manuals for authorised officers and system operators.

4.0 The systems

4.1 The Council owns and operates overt CCTV surveillance systems which cover key public spaces including town centres and council offices. The current CCTV systems are:

- Fixed CCTV system across public spaces and town centres in the borough.
- Council Office CCTV system covering internal and external public spaces around council buildings.
- Body Worn Video Cameras (BWVC).
- Vehicle mounted video camera systems (VMVC).
- Leisure Centres CCTV system covering internal and external public spaces.

4.2 The cameras, as part of the systems noted above will not be hidden (they will be overt systems) and signs saying that cameras are operating in and around the surveillance areas are displayed in visible locations.

4.3 A central register of all surveillance camera systems will be maintained by the Senior Responsible Officer (SRO). All Services will need to ensure that they provide information necessary to ensure that the register is complete and up-to-date.

5.0 Monitoring and Recording Facilities (excluding VMVC and BWVC)

5.1 A staffed monitoring room for the Council's town centre and public open spaces cameras is located within a secure Council owned and controlled building and is known as the 'CCTV Control Room'. The CCTV Control Room

is staffed by specially selected and trained operators and access to the CCTV Control Room is limited to authorised personnel only. The CCTV Control room is managed by the Community Protection Manager who is the Single Point of Contact (SPOC) in respect of surveillance systems.

5.2 For all other Council surveillance camera systems a secure Council controlled monitoring room is used. Access to these controlled rooms is limited to authorised personnel who have been specifically selected and trained in respect of the system and the monitoring of the system and handling of data. .

5.3 For the purpose of this policy, a control room is any area or room (including the CCTV Control Room) which contains equipment that forms part of a surveillance system which stores the recorded material captured.

5.4 No equipment, other than that housed within a control room shall be capable of recording images from any of the surveillance cameras.

5.5 All viewing and recording equipment shall only be operated by trained and authorised users with other access limited to those who require it for a specific legitimate reason and where permission has been given by the Single Point of Contact for surveillance cameras.

5.6 CCTV operators are able to record images from selected cameras in real-time, produce hard copies of recorded images, replay or copy any pre-recorded data in accordance with this Policy (para 8), relevant Codes of Practice and where necessary in accordance with the law.

5.7 All operators shall receive training relevant to their role in the requirements of the relevant legislation and the Codes of Practice and this policy. Ongoing training will be provided as necessary, refresher training will also be provided periodically to remind operators of the relevant legislation.

6.0 Monitoring and Recording facilities – VMVC and BWVC

6.1 All footage and images recorded on VMVC and BWVC are recorded to an internal memory within each individual device. The operation of these cameras will be in accordance with the operational guidance for those camera systems and those cameras will only be operated by those authorised officers who have been trained in the operation of the cameras.

6.2 Any recording or monitoring of images captured from VMVC and BWVC will be undertaken by authorised personnel within the relevant service areas and the images will only be viewed for a legitimate purpose in accordance with this policy and the Codes of Practice.

7.0 Security and retention of recorded material

7.1 All surveillance camera material shall be stored securely and protected by appropriate security measures to safeguard against unauthorised access and use.

7.2 Images and information obtained from the surveillance camera system shall be stored no longer than that which is strictly required for the stated purpose of the system's use. **This will ordinarily be no longer than 28 days**.

7.3 The Council's corporate Records and Retention Policy indicates that CCTV footage will be retained until overwritten unless required for use in legal proceedings, in which case the CCTV footage will become part of the case file and stored in accordance with the Records and Retention Policy.

7.4 Information must be securely destroyed once its purpose has been discharged and at the end of its retention period unless there is a documented reason to retain it (e.g. to support legal proceedings).

7.5 Deleted information shall not be capable of being recovered. ICT shall be consulted on the appropriate method of deletion.

8.0 Access to Information

8.1 Any request for images or information from the Council's surveillance camera systems by individuals through a subject access request or by a third party organisation under the Data Protection Act 2018 should be requested in writing and forwarded to Legal Services to consider whether the release of information is lawful.

8.2 Any request for information from the Council's surveillance camera systems made under the Freedom of Information Act 2000 should be in writing and should be forwarded to Legal Services to consider whether the release of information is lawful.

8.3 From time to time the Council receive requests for access to information from surveillance cameras from the police. Such information will often fall under an exemption to the Data Protection Act 2018 as it is required for the prevention or detection of crime or the apprehension or prosecution of offenders. Where the police request information from the CCTV Control Room, the SPOC can authorise release of footage where necessary and in compliance with the law. For all other control rooms where requests for CCTV are made by the Police, the relevant system manager should forward the request to Legal Services.

8.4 No surveillance camera information should be disclosed to a third party unless in accordance with this policy and the Data Protection Act 2018.

8.5 Records of all disclosures of surveillance camera information disclosed to third parties should be maintained.

8.6 Whenever disclosure of information from surveillance camera systems is undertaken, steps should be taken to ensure that the method of disclosure is secure, and information is only seen by the intended recipient. Consideration should also be given as to whether images or parts of images need to be obscured to prevent unwarranted identification and limit unfair intrusion into the privacy of individuals.

9.0 Privacy

9.1 All overt surveillance camera systems should be included in the Council's Information Asset Registers and referred to in the Council's registration with the Information Commissioner under the Gedling Borough Council Registration.

9.2 Each system identified within 4.1 has appropriate restrictions on the data it captures and is in accordance with the purpose of the system. This includes regular auditing of the images each camera captures in all of the systems the Council owns to ensure privacy, compliance and appropriateness.

9.3 Every consideration will be given to the right of the general public and staff to go about their daily business without fear of their loss of privacy.

9.4 Cameras will not be used to look into private residential property. Where the equipment permits it 'Privacy zones' will be programmed into the system as required in order to ensure that the interior of any private residential property, within range of the system, is not surveyed by the system. If such 'zones' cannot be programmed the operators will abide by the appropriate legislation with regards to privacy issues.

9.5 Appropriate signage must be in place in respect of all surveillance systems to ensure that the public are aware that such systems are in operation. The operation of such systems will also be referenced in the Council's privacy notices.

10.0 System evaluation

10.1 As stipulated in the Surveillance Commissioner's Code of Practice, an annual review and audit of the surveillance camera systems will be completed and published to ensure that the purpose of the systems and objectives are being complied with and achieved. The report will include:

- An assessment of the impact upon crime and anti-social behaviour of the system;
- An audit of the compliance with this policy including whether any footage viewed and/or downloaded was in line with the system aims and objectives; and,
- Any operational changes made over 12 months, including the

addition or removal of cameras.
- An assessment of the technical capability of the systems to ensure they remain fit for purpose.

10.2 The production of the Annual Review will be the responsibility of the System Manager/s to organise and may include independent undertakings by an appropriate third party organisation e.g. another local authority.

10.3 The SRO will report annually to Members on the outcome of audits and reviews and any amendments required to this policy document.

10.4 Operational changes to the systems will be approved by the SRO. This will include any additional cameras, or removal of cameras. Considerations of these changes will include:

- Whether the changes would meet all legal requirements necessary; and,
- A review of other tools and powers used to address the issue or concern.

11.0 Complaints

11.1 The Council's complaints procedure will apply to the handling of complaints related to surveillance camera operation. Complaints of this nature should be referred to the SPOC who will, where necessary, liaise with the Data Protection Officer in relation to data protection issues that are raised. Departments operating surveillance cameras may be asked to provide information to the SPOC or the SRO.

11.2 Complaints may be handled as a data protection complaint if the complaint relates to the use of personal information. Such complaints should be notified as soon as possible to the Data Protection Officer and within 24 hours at the latest.

11.3 Where complaints cannot be resolved through the internal complaints process they may be referred to the Information Commissioner's Office or the Local Government and Social Care Ombudsman as appropriate.

11.4 Any data breach arising out of the processing of personal information captured through the Council's surveillance camera systems should be reported immediately to the Council's Data Protection Officer and in any event within 24 hours of the breach occurring. Officers should have regard to the Council's breach reporting process as set out in the Council's Information Security Policy.

12.0 Roles and Responsibilities

12.1 The Senior Responsible Officer for surveillance cameras is the Director of Organisational Development and Democratic Services.

12.2 The Legal Services Manager is the Data Protection Officer and is responsible for ensuring compliance with the relevant legislation and conducting audits of the system.

12.3 The Community Protection Manager is the Single Point of Contact for all operational and monitoring queries in respect of surveillance cameras systems and is responsible for day to day operational management of the CCTV control room.

12.4 Information Asset Owners (Service Managers) are accountable for ensuring that surveillance camera systems operating as part of their service's business, do so in accordance with the provisions of this policy. Specifically, they will:

- Ensure that planning for any new Surveillance camera systems is informed by a DPIA and that the DPIA is approved before the system becomes operational.
- Approval is obtained from the SRO for any new surveillance cameras or systems.
- Assign a Surveillance Camera System Owner to be responsible for the oversight of all new and existing systems. This maybe, but is not required to be, the Information Asset Owner for the business area undertaking the surveillance.
- Conduct an annual review and audit of surveillance camera systems.

12.5 Responsibility for the implementation of this and associated procedures and for reporting performance issues related to surveillance camera systems rests with all employees who have involvement in the management of the surveillance camera equipment.

12.6 Staff who use the CCTV system have the following responsibilities:

- To uphold the arrangements of this policy and associated Codes of Practice.
- To handle images and data securely and responsibly, within the aims of this Policy.
- To be aware that they could be committing a criminal offence if they misuse surveillance camera images.
- To uphold the corporate procedure for subject access requests.
- To report any breach of procedure to the Data Protection Officer using the Council's data breach process
- To attend training / refresher sessions as required.
- To assist and co-operate any surveillance system audits and reviews.