APPENDIX B

# Selby District Council

## Overt Surveillance Policy

# Document Control

| | |
|---|---|
| **Document Control Organisation** | **Selby District Council** |
| **Title** | **Overt Surveillance Policy** |
| **Subject** | **Information Governance** |
| | |
| **Version** | **0.4** |
| **Publication Date** | **1/10/2021** |
| **Last Reviewed Date** | **N/A** |
| **Next Review Date** | **1/10/2022** |

## Policy Version History

| Version | Date | Notes | Author |
|---|---|---|---|
| 0.1 | 15/11/2019 | Initial draft | Veritau DPO |
| 0.2 | 05/12/2019 | Inclusion of Lone Worker section | Veritau DPO |
| 0.3 | 21/01/2021 | Completion of some amendments due to feedback received plus format changes. | Veritau DPO |
| 0.4 | 25/8/2021 | Draft Amendments to align with other Council policies including refreshed Corporate Policy: RIPA | Alison Hartley Solicitor to the Council |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

**Update and approval**

This Policy shall be updated annually or, if deemed necessary, whenever there is a need or requirement to do so. It will be updated in respect of changes within the privacy field, other regulatory changes, changes in the market where the District Council operates and internal changes within the District Council. Any changes to this Policy are subject to approval by the SIRO.

# Contents

# 1. Introduction

This policy forms part of the Council's wider Information Governance Framework.

This policy is concerned with the use and governance of surveillance technology, and the processing of Personal Data which has been collected by using surveillance technology. The policy sets out the standard to ensure the Council complies with the Data Protection Act 2018 and UK GDPR as well as the Surveillance Code of Practice.

Queries about any aspect of the Council's Information Governance strategy or corresponding policies are to be directed to the Data Protection Officer (DPO) at: information.governance@veritau.co.uk

# 2. Scope

*Who the policy applies to*

This policy applies to all Council officers, any authorised agents working on behalf of the Council, including temporary or agency staff, elected members, volunteers, and third party contractors. The Policy does not apply to Selby traded companies as these organisations are data controllers in their own right and are therefore obliged to have their own information governance policies.

For the benefit of doubt this Policy will refer to all individuals within scope of the policy as 'Officers'. Officers who are found to knowingly or recklessly infringe this policy may face disciplinary action in accordance with the Council's disciplinary policies and procedures.

*What the policy applies to*

Surveillance is the monitoring of behaviour, activities, or other changing information for the purpose of influencing, managing, directing, or protecting people. Unless stated otherwise, this policy will apply to any surveillance used by the Council.

The policy does not apply to 'covert' surveillance or to social media surveillance as these are covered by the *Corporate Policy: Regulation of Investigatory Powers*[1]

Key Messages

[1] Covert Surveillance can be defined as any surveillance deliberately conducted without the knowledge of the individual(s) who are being monitored. [insert link to Corporate Policy: RIPA here]

1. Officers will ensure that CCTV systems are planned, maintained, and operated within the provisions of data protection legislation and this policy. Such systems must have a specified purpose and only be used for the specified purpose.

2. The Council may use audio equipment to record internal or external meetings. Those being recorded by such equipment must be made aware of this prior to the recording taking place otherwise this constitutes 'covert' surveillance which can only be permitted in certain circumstances.

3. The Council operates tracking location devices in its fleet vehicles. Officers must be made aware of such devices prior to the use of that vehicle.

4. All Council operated surveillance systems must be registered centrally and reviewed every two years.

# 3. CCTV Systems

*Planning CCTV Systems*

Any new implementation of CCTV systems will employ the concept of 'privacy by design' which will ensure that privacy implications to data subjects will be considered before any new system is procured. The prescribed method for this is through the completion of a Data Protection Impact Assessment (DPIA). Officers should use the DPIA process as defined by the Council *Personal Privacy Policy*[2].

The Council has various statutory responsibilities to protect the privacy rights of data subjects. Therefore during this planning phase officers need to consider and address the following:

1. The purpose of the system and any risks to the privacy of data subjects.

2. That there are statutory requirements placed on the location and position of cameras. This means that cameras must be positioned to meet the requirement(s) of the intended purpose(s) and not exceed the intended purpose(s).

3. The obligation to ensure that the CCTV system can meet its intended purpose(s) also means that the system specification must be such that it can pick up any details required for these aims. For example the system must record with sufficient resolution to perform its task.

[2] [insert link to Personal Privacy Policy policy here]

4. The system must also have a set retention period (the typical retention period is one month) and, where appropriate, the Council must also have the ability to delete this information prior than the set retention period in order to comply with the rights of data subjects.

5. That the Council will need a level of access to the system and there will need to be the option to provide other agencies (such as law enforcement agencies) with specific footage if requested. If a data subject is captured and recorded by the system, then that individual also has the right to request a copy of that footage under subject access provisions.

As per the Council's Personal Privacy Policy[3], officers will ensure that a contract will be agreed between the Council (as Data Controller) and the CCTV system provider. Consideration should also be given to whether there are any joint data controller arrangements where the system is shared with another organisation. Data Processing clauses must be included within the written contract.

*CCTV Privacy Notices*

The processing of personal data requires that individuals that the data relates to - which in this case any individuals captured by the CCTV system, are made aware of the processing taking place.

As such the use of CCTV systems must be visibly signed. This signage will include the purpose for the system (e.g. the prevention or detection of crime), the details of the organisation operating the system and who to contact about the system (including basic contact details). The signage must be clear enough that anyone entering the recorded area will be aware that they are being recorded.

A more detailed Privacy Notice[4] for the use of CCTV will be maintained with the intention of informing data subjects of their rights in relation to surveillance data. Officers should refer to the Council's Personal Privacy Policy regarding this notice.

*Access to CCTV Footage*

CCTV footage will only be accessed to comply with the specified purpose, for example if the purpose of maintaining a CCTV system is to prevent and detect crime then officers must only examine footage where there is evidence to suggest criminal activity having taken place

A central register of surveillance systems will be maintained by the Council.[5] Each CCTV system will have an Information Asset Owner who will be responsible for the governance and security of the system. The Information

[3] [insert link to Personal Privacy Policy] [
[4] insert link to SDC Privacy Notice CCTV V0.2]
[5] [insert link to the Councils Central Register of Surveillance Systems]

Asset Owner will authorise officers to access CCTV footage either routinely or on an ad-hoc basis.

*CCTV Footage Disclosures*

Requests by individuals for CCTV recordings should be regarded as subject access requests. Officers should refer to the Information Access and Information Rights Policy Version1.0 21/1/[6] when considering such requests.

Requests by other agencies, including law enforcement agencies, for CCTV Recordings should be considered under the terms of the North Yorkshire Multi Agency Information Sharing Protocol[7] which the Council is a signatory to.

*Review of CCTV*

CCTV systems must be reviewed biennially to ensure that systems still comply with Data Protection legislation and national standards. Officers should use the checklist included in Appendix One of this policy to complete this review.

It is the responsibility of the Information Asset Owner to ensure reviews are completed and evidence of the reviews taking place are recorded on the corporate register of surveillance systems

# 4. Audio and Video Recordings

*Systematic Use of Audio and Video Recordings*

Systematic recordings may be used by the council where it is considered proportionate to the aims of the recording, for example the recording of council committee meetings for the purposes of promoting accountability and public engagement.

Any new systematic use of recording will require that a DPIA is conducted. With any recording the scope of the recording and whether data subjects can choose not to consent to the recording must be established during the DPIA stage.

Recordings must only be accessed where there is a valid reason to do so – for example for law enforcement purposes or to fulfil the purpose that the information was created for.

[6] [insert link to the Councils Information Access and Information Rights Policy]
[7] [insert link to North Yorkshire Multi Agency Information Sharing Protocol]

Before recording begins, data subjects must be informed that they are going to be recorded. If, legislation permitting, data subjects have the option not to consent to the recording, then they should be given the choice and possible alternative. This information can be given verbally, so, for example, individuals can be informed as part of a phone call recording. However, a more detailed written privacy notice must exist that an individual can be referred to. The verbal privacy notice will at least include the purpose for the recording, any alternative available, and that more information is available on the Council's website. The written privacy notice will also include details of the data subject's data protection rights and the ensilaged retention period and/or criteria.

The recording device or software must be able to produce good quality recordings so that the recordings are fit for the purpose for which they are made. Copies should be made available to data subjects upon request unless there is a legislative permitting reason not to do so. Officers should refer to the Information Access and Information Rights Policy [8] when handling such requests.

*Ad-Hoc Use of Recordings by Officers*

Although officers do not require the consent of members of the public to use audio recording equipment on an ad-hoc basis, so long as there is a lawful and justified reason for doing so, it is not permissible to record members of the public either using Audio or Video without their knowledge unless this has been authorised through the 'Regulation of Investigatory Powers Act" and in accordance with the Council's *Corporate Policy: Regulation of Investigatory Powers*[9]

*Recordings submitted by members of the Public*

Members of the public may submit recordings to the Council. However, members of the public that submit such recordings must be made aware that they may not be submittable as "evidence" and that this is left to the discretion of relevant officers. Reasons for not permitting the submission of a recording could be that the recording is not of good enough quality or that there are concerns that recordings have been altered at a later stage.

[8] Link to Information Access and Information Rights Policy]

[9] [Link to Corporate Policy: Regulation of Investigatory Powers

## 5. Fleet Management Vehicle Surveillance

*Location data*

The Council's fleet cars are fitted with devices that record the location of the vehicle. Where there is suspicion of inappropriate conduct, managers will have permission to access these records to investigate the suspicions.

Members of staff who use fleet cars are made aware of this when they are granted the use of a fleet car and agree to the terms and conditions of using fleet cars. As well as the terms and conditions a short notice will be visible in the vehicles. This short 'just in time' notice will signpost to a comprehensive privacy notice on the Council's website.

## 6. Lone Worker activation phone application

*Personal details and location Data*

The employee's Smartphone will have an Application installed on their phone which allow an employee to activate an alarm in an emergency situation. The data collected will only be utilised in order to help safeguard the individual and will at no time be used as part of any performance review of the employee in question.

It is possible for the Council to ping the Smartphone which would reveal the employee's location if the application has been left running in the background. This does not allow the Council to track the employee.

Members of staff who use Smartphones with the Application installed, will be made aware of this when they sign up to the use of the Application and agree to the terms and conditions of using the Application. Whilst also considering the terms and conditions, the employee will also be provided with information which will signpost them to a comprehensive privacy notice on the Council's website.

## 7. Related Documents

Officers who are planning the implementation of a surveillance system are encouraged to read the following related documents prior to implementation:

- Data Protection Impact Assessment Template (intranet link)

- ICO Surveillance code of Practice (External Link)
- Surveillance camera code of practice - GOV.UK (www.gov.uk)

## Appendix One: Surveillance System Review Checklist

*This checklist should be used by officers when conducting the mandatory biennial review of surveillance systems. This checklist needs to be signed off by the relevant information asset owner.*

| **Name and Description of Surveillance System:** | | |
|---|---|---|
| The purpose and requirements of the system are addressed by the system (i.e the cameras record the required information) | **YES** | **NO** |
| | **Notes:** | |
| The system is still fit for purpose and produces clear images of adequate resolution. | **YES** | **NO** |
| | **Notes:** | |
| Cameras are sited in effective positions to fulfil their task. | **YES** | **NO** |
| | **Notes:** | |
| Cameras are positioned so that they avoid capturing the images of persons not visiting the premises and/or neighbouring properties. | **YES** | **NO** |
| | **Notes:** | |
| There are visible signs showing that CCTV is in operation. These signs include:<br>▪ Who operates the CCTV,<br>▪ Their contact details,<br>▪ What the purpose of the CCTV is. | **YES** | **NO** |
| | **Notes:** | |
| CCTV recordings are securely stored and access limited. | **YES** | **NO** |
| | **Notes:** | |

| | | |
|---|---|---|
| The system has the capability to transfer recordings to law enforcement or to fulfil a request for an individual's own personal information. | **YES** | **NO** |
| | **Notes:** | |
| The system has a set retention period. This retention period should only be long enough to fulfil the CCTV's purpose and not longer. Outside of this retention period information should be deleted | **YES** | **NO** |
| | **Notes:** | |
| The system users should be able to selectively delete information still inside the retention period to fulfil the right to erasure. | **YES** | **NO** |
| | **Notes:** | |
| All operators have been authorised by the Information Asset Owner and have sat their mandatory data protection training. | **YES** | **NO** |
| | **Notes:** | |
| This system has been declared on the corporate register of surveillance systems. | **YES** | **NO** |
| | **Notes:** | |

| | |
|---|---|
| **Checklist Completed By:**<br><br>Name:<br>Job Title:<br>Date: | **Checklist Reviewed and Signed By (Information Asset Owner):**<br>Name:<br>Job Title:<br>Date: |