CLACKMANNANSHIRE COUNCIL

THIS PAPER RELATES TO ITEM 10

ON THE AGENDA

Report to Council

Date of Meeting: 17th December 2015

Subject: Use of Overt Surveillance Systems Policy

Report by: Head of Resources and Governance

1.0 Purpose

1.1. The purpose of this report is for the Council to consider and agree a policy for the use of Overt Surveillance Systems.

2.0 Recommendations

2.1. To agree to the adoption of Overt Surveillance Equipment Policy (Appendix A).

3.0 Considerations

3.1. The Council already has a number of Closed Circuit Television (CCTV) systems and could, in the appropriate circumstances, utilise other overt surveillance technologies. The use of such technologies may have an impact on people's right to live and work in private as they capture personal information about them and so impact on their privacy. Therefore the Council must have the proper governance arrangements in place via a policy and appropriate guidance to ensure compliance with both the Data Protection Act 1998 and the Human Rights Act 1998.

3.2. The use of CCTV has been around for a number of years and the number of related technologies is rapidly increasing. This has been reflected in the Information Commissioner Office recently updating their Code of Practice from its original version in 2008 to capture these developments.

3.3. The Council's CCTV systems capture personal images of both employees and members of the public so it must ensure that the appropriate practices are put in place to comply with the eight Data Protection Act principles. While there are a number of local controls and processes in place there is no Council-wide approach and therefore limited controls on the use of overt surveillance systems. Details on the location of the Council's CCTV cameras are proposed to be published on ClacksWeb.

3.4. The use of overt surveillance technology provides a number of benefits such as minimising expenditure due to vandalism, protecting staff and customers from criminal activity and effectively and efficiently delivering some services. This policy also links to the council's personal safety and managing unacceptable behaviour policies.

3.5. The Information Commissioner has a code of practice for using these types of surveillance systems. The Council's policy and supporting documentation has been designed to comply with this code in practice and spirit.

3.6. Prior to the procurement and deployment of any new overt surveillance systems or the deployment of existing technologies to new environments the Policy states that agreement must be sought from the relevant Service Committee to enable elected members to have oversight of the use of overt surveillance in Clackmannanshire.

3.7. This policy does not include covert surveillance. The use of covert surveillance is covered by the Council's policy detailing the procedures to be followed and the extent of the Council's powers under the Regulation of Investigatory Powers (Scotland) Act 2000.

4.0 Conclusion

4.1. The policy will allow officers the opportunity to use overt surveillance system, where it can be justified, in a safe manner and in line with the Council's statutory requirements. The Policy also takes account of the future deployment of new or emerging technologies. The policy is supported by guidance documents and sets out that each installation or use of a surveillance system must have a management control document in place. The control document sets out the specifics of how the system is used, for what purpose and the controls in place.

5.0 Sustainability Implications

5.1. There are no sustainability implications.

6.0 Resource Implications

6.1. Financial Details

6.2. There are no financial implications to this policy.

6.3. Staffing

6.4. The impact on staffing is minimal in the completion of the appropriate paperwork, both historic as systems are reviewed and prior to any new set up.

7.0 Exempt Reports

7.1. Is this report exempt? Yes ☐ (please detail the reasons for exemption below) No ☑

8.0 Declarations

The recommendations contained within this report support or implement our Corporate Priorities and Council Policies.

(1) **Our Priorities** (Please double click on the check box ☑)

The area has a positive image and attracts people and businesses ☐

Our communities are more cohesive and inclusive ☐

People are better skilled, trained and ready for learning and employment ☐
Our communities are safer ☑
Vulnerable people and families are supported ☐
Substance misuse and its effects are reduced ☐
Health is improving and health inequalities are reducing ☐
The environment is protected and enhanced for all ☐
The Council is effective, efficient and recognised for excellence ☑

(2) **Council Policies** (Please detail)

9.0 Equalities Impact

9.1 Have you undertaken the required equalities impact assessment to ensure that no groups are adversely affected by the recommendations? Yes ☐
No ☑

10.0 Legality

10.1 It has been confirmed that in adopting the recommendations contained in this report, the Council is acting within its legal powers. Yes ☐

11.0 Appendices

11.1 Please list any appendices attached to this report. If there are no appendices, please state "none".

Appendix A draft Overt Surveillance equipment policy

12.0 Background Papers

12.1 Have you used other documents to compile your report? (All documents must be kept available by the author for public inspection for four years from the date of meeting at which the report is considered)
Yes ☑ (please list the documents below) No ☐

The Information Commissioners Code of Practice on the Use of Overt Surveillance Systems.

Author(s)

NAME	**DESIGNATION**	**TEL NO / EXTENSION**
Andrew Hunter	Senior Governance Officer	

Approved by

NAME	**DESIGNATION**	**SIGNATURE**
Stephen Coulter	Head of Resources & Governance	[redacted]
Nikki Bridle	Depute Chief Executive	[redacted]

Appendix A

Clackmannanshire Council

Use of Overt Surveillance Equipment Policy

Introduction

This policy sets out the Council's position in relation to the use of Overt surveillance systems.

Overt surveillance Systems (OSS) used to be restricted to a camera in a fixed point but they now include cameras that can move around the area they cover by remote control, body worn videos (BWV) including audio recording, automatic number plate recognition cameras and unmanned aerial systems (UAS). Additionally other everyday devices can also be used in this manner such as mobile phones and tablets.

The capturing of images by OSS can impact on an individual's right to privacy because of the collection of their personal data.

This policy is designed to ensure that the Council protects data subjects' privacy and complies with its requirements under the Data Protection Act 1998.

This policy and supporting documentation, practices and recommendations have been created in line with the legislation and following the Information Commissioner's Code of Practice on Surveillance Cameras.

While the Council doesn't currently have or deploy all of these types of OSS, the document covers the policy considerations before authorisation is given to their use should such equipment ever be deployed in the future.

1. The Purposes of Overt Surveillance System Deployment

The purpose must be for one of the following reasons:-

- The prevention or detection of crime
- To ensure public and/or staff safety
- The protection of public assets
- To support the Council's regulatory functions

2. System Set Up and Management

Every OSS set up, installation or operational deployment requires to have specific controls in place set out in the Management Control Documents appended to this policy.

Each installation or set up must have a designated responsible officer and service who manage all aspects of the system while it is operational.

Prior to installation and/or when deciding on whether to install/continue to use OSS, an impact assessment (including impacts on privacy) must be carried out and the situation regularly reviewed.

Each Management Control Document must address the following key principles.

- Audio recording should only be used in very limited circumstances and should be clearly set out in both the Management Control Document and any signage.
- Mobile video recorders are likely to also record audio. Given the additional intrusive nature of this type of recording, the management document must detail the circumstances when the camera will be deployed.
- Appropriate signage must be put in place to let people know that they are in an area that is covered by OSS. Again any audio recording must contain additional clear signage.

4. Deployment of Cameras

Every Management Control Document must include where cameras will be sited, what they will cover and why they are located where they are. If the cameras are mobile then consideration of how and where they will be deployed must be considered every time they are used.

5. Procedures on Use, Storing and Viewing

Every OSS must have written procedures on how it will be used and who can use/access the system.

Each set up must have appropriate measures to securely store recordings (both images and audio), destroy after an appropriate time and record who accesses images and at which times. All access to recordings must be shown to be both necessary and proportionate. The designated responsible officer must maintain a record of all access requests.

Images are considered to be personal data and as such, data subjects are entitled to access images about themselves. Any request for images by data subjects should follow the Council's Data Protection Policy and guidance on subject access requests.

How images will be viewed must also be clearly set out, for example, can they be watched live or are they purely recorded. If monitor screens are used it must be ensured that they can't be seen by the general public.

6. Retention and Destruction of Images

There is not a specified minimum or maximum retention period set out in the Data Protection Act. Every installation or setup and its purpose will need to be considered before judging how long images should be retained. Each

Management Control Document must clearly set out how long recordings will be retained and the method for disposal.

7. Security of images

All images should have the appropriate technical, organisational and physical security in place as per current Council standards or the ICO code of practice. All measures should be recorded in the Management Control Document.

8. Staff who access or manage surveillance camera systems

All staff who use or have access to OSS, should ensure they are fully aware of this policy, the Information Commissioner's Code of Practice for Surveillance Cameras and Personal Information, the Council's guidance document and the Management Control Document for their OSS deployment.

They should also know how to handle recordings securely and what to do if requested for images, for example from the police.

Staff should be aware that they could be committing a criminal offence if they misuse surveillance camera recordings.

8. Covert uses of Surveillance Cameras

This policy does not cover covert surveillance which is managed under the Council's policy on covert surveillance.

9. Central Register of Management Documents

Resources and Governance will maintain a central record with a copy of all Management Control Documents on behalf of the Council. These will be managed in accordance with the Council's Records Management Policy.

10. Maintenance and Auditing

Each OSS must have procedures in place to ensure the maintenance and performance of the system, including setting of date/time stamps.

Clear processes are required for the auditing of the system and who this will be done by.

11. Notification to the Information Commissioner

The Council's notification to the Information Commissioner will include details of its uses of OSS to comply with the Data Protection Act 1998.

Resources and Governance will be responsible for ensuring that the Council's notification is kept up to date.

12. Oversight

A proposal to introduce any new form of surveillance technology or to introduce existing technologies to new environments will need to be agreed by the relevant Service Committee prior to deployment. Service Committees should also ensure that they receive reports about the ongoing use of OSS to ensure that their use is proportionate and in line with this Policy.

13. Policy Review and Enquiries

A review of this policy will be completed every three years from the date of first publication.

Enquires should be directed to:

Head of Resources and Governance
Clackmannanshire Council
Kilncraigs
Greenside Street
Alloa
FK10 1EB

or e -mail
democracy@clacks.gov.uk

Management Control Document of Surveillance Camera System

Insert Name of System

SERVICE RESPONSIBLE	
DESIGNATED RESPONSIBLE OFFICER	
DATE CREATED	
SYSTEM CONTROLLED BY	EG CLACKMANNANSHIRE COUNCIL

TYPE OF SYSTEM: include make and specifications
**Delete as appropriate* Does the system have facilities for audio recordings - Yes/No Can it be controlled separately or disabled from video recordings - Yes/No

AREA COVERED BY THE SURVEILLANCE SYSTEM
(Insert Plan or Map where appropriate)

POTENTIAL DATA SUBJECTS RECORDED BY THE SURVEILLANCE SYSTEM

PURPOSE OF THE SURVEILLANCE SYSTEM
EG PREVENTION AND DETECTION OF CRIME AND PUBLIC SAFETY WHY IS THIS THE MOST SUITABLE MEDIUM FOR THIS PRUPOSE?

PROCEDURES ON HOW SYSTEM WILL BE USED
CAN BE ATTACHED AS AN APPENDIX

MAINTENANCE ARRANGEMENTS

NAME	
ORGANISATION	
ANY CONTRACTUAL ARRANGEMENTS	YES/NO
CONTRACT DETAILS	

LOCATION OF CAMERAS

HOW WILL THE SYSTEM BE USED?
Storing and viewing the images

LOCATION AND DEPLOYMENT OF SIGNAGE

DETAILS OF ANY POTENTIAL COLLATERAL INTRUSION

ACCESS TO IMAGES

REQUESTS MADE TO	
NAME	**EMAIL**
DESIGNATION	**PHONE NUMBER(S)**

REQUESTS MADE TO	
NAME	**EMAIL**
DESIGNATION	**PHONE NUMBER(S)**

REQUESTS MADE TO	
NAME	**EMAIL**
DESIGNATION	**PHONE NUMBER(S)**

RETENTION SCHEDULE
How will the data be stored? For how long? Why it needs to be kept for this length of time? How will it be destroyed?

REVIEW SECTION

Reviews should include compliance checks, eg are retention periods being complied with. The review timescales should be done as often as needed for any particular installation, but should be at least annually.

DATE OF LAST REVIEW	REVIEW CONDUCTED BY

SECURITY MEASURES

List the security measures that are in place with this set up, eg system saves data direct to Council secure network, encryption is automatically installed to the physical set up, devices have password security to any organisational standards, local procedures for staff.

Technical
Organisational
Physical

IMPACT ASSESSMENT

INSERT IMPACT ASSESSMENT

Authorisation

The Management Control Document should be signed by either a Head of Service or appropriately delegated Service Manager.

Signature	
Print	
Date	

The control document also must be signed by the Head of Resources and Governance.

Signature	
Print	
Date	