REPORT TO: CORPORATE COMMITTEE ON 23 APRIL 2024

SUBJECT: CLOSED CIRCUIT TELEVISION POLICY

BY: DEPUTE CHIEF EXECUTIVE (EDUCATION, COMMUNITIES AND ORGANISTIONAL DEVELOPMENT)

1. REASON FOR REPORT

1.1 To request the Committee to consider and approve a new Council wide Closed Circuit Television (CCTV) Policy.

1.2 This report is submitted to Committee in terms of Section III (B) (40) of the Council's Scheme of Administration relating to ensuring suitable framework is in place for performance management across the Council.

2. RECOMMENDATION

2.1 It is recommended that the Committee considers and approves the new CCTV Policy as set out in APPENDIX 1 and summarised in Section 4 below.

3. BACKGROUND

3.1 The Council has numerous internal and external CCTV cameras and systems throughout the Council's estate, including in schools, libraries and offices, as well as in public areas. These CCTV cameras gather images of people, places and events.

3.2 CCTV is used for a range of purposes including: promoting and supporting community safety, protecting Council property and assets, creating and supporting a safe environment for employees and the public within Council properties and public areas, traffic management, and, preventing and detecting crime.

3.3 The Council must ensure that images captured by CCTV systems are managed in accordance with legislation, including Human Rights Legislation and Data Protection Legislation.

3.4 This CCTV Policy will be applicable to all Council owned CCTV systems, and will supersede any policies devised by individual departments or services. This Policy aims to bring a unified approach and standardise CCTV governance to improve the existing management of CCTV systems across the Council.

3.5 Due to the overarching corporate nature of the Policy, the Council's Information Assurance Group have taken the lead on producing this Policy, with relevant departments contributing significantly to its creation.

3.6 CCTV footage that identifies and relates to an identifiable individual is considered personal data and must be handled in accordance with Data Protection legislation. The Information Commissioner's Office (ICO) is responsible for monitoring and enforcing UK Data Protection legislation; they provide advice, produce guidance and, have the power to prosecute and penalise individuals and organisations for poor compliance with Data Protection.

3.7 The CCTV Policy does not cover Public Space CCTV systems. These systems are owned and maintained by the Council, but are monitored and operated by Police Scotland. As such, Police Scotland's Policies would be applicable for these systems.

3.8 This Policy does not cover:

- the use of equipment as part of any covert surveillance operation that has been authorised in terms of the Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA); these operations are subject to separate RISPA policies and procedures.
- the capture of audio by CCTV systems; no audio is captured by Council CCTV systems.

4. HIGHLIGHTS FROM THE COUNCIL'S CCTV POLICY

4.1 The CCTV Policy applies to all Moray Council employees and all third party providers acting on behalf of the Council. It ensures that all Council employees and contractors will be aware of their obligations in relation to the data captured on CCTV systems. The Policy endeavours to cover the Council's current CCTV situation, aims to clarify and define roles and responsibilities in the use of CCTV, and, standardise governance elements, including:

- a new requirement for all CCTV cameras and systems to be recorded on a central register (managed by Property Services),
- a stated requirement that staff training is provided;
- a stated requirement that procedures are in place verifying how each system will be accessed, monitored and shared; all training within service operating procedures should also include training on the Human Rights Act 1998 with regard to Article 8 in particular and the requirements of RIPSA,
- a stated requirement for Services to review CCTV operating procedures annually.
- a stated requirement that images captured will comply with the Council's Retention Schedules, with service operating procedures specifying the particular retention cycles applicable to each CCTV system.

4.2 Services responsible for the operation of a CCTV system will also need to:

- Complete a Data Protection Impact Assessment (DPIA) for their CCTV systems, to ensure that Data Protection risks have been identified and mitigated,

- Ensure that CCTV signage is clearly and prominently placed at entrances and within the CCTV coverage areas, and, that the link to the Council's CCTV Privacy Notice is included on all Council CCTV signage,
- Maintain detailed records when disclosing captured images to third parties, and,
- Ensure that there are up-to-date procedures for each system, with staff fully aware of the requirements.

4.3 Images captured by the Council's CCTV systems should not be disclosed to any third party, unless there is a lawful basis to do so. Requests regarding the transfer of CCTV data will be handled on a case by case basis in the same manner as requests for personal data. As such, any such request, for example from a third party such as Police Scotland, will generally require the submission of a completed Data Protection Release Request form, setting out the data requested and the legal basis for disclosure before any personal data can be released.

4.4 Images of identifiable individuals captured by the Council's CCTV systems may need to be released to satisfy a Subject Access Request (SAR) made under Data Protection legislation. These requests will be processed as per the current centralised method, with stills of videos released to allow for suitable redaction. SARs for images captured on Public Space CCTV must be made directly to Police Scotland.

4.5 The Council receives numerous Freedom of Information (FOI) requests every year regarding CCTV. Holding information about CCTV in a central register will ultimately save staff time when responding to such FOIs.

5. SUMMARY OF IMPLICATIONS

(a) Corporate Plan and 10 Year Plan (Local Outcomes Improvement Plan (LOIP))
None

(b) Policy and Legal
None

(c) Financial implications
There are no financial implications arising from this report, however the promotion and implementation of effective CCTV governance impacts positively on the Council's ability to mitigate its exposure to financial risk, particularly monetary penalties levied by the ICO for data breaches. For serious breaches of Data Protection legislation the ICO have the power to issue fines of up to £17.5 million.

(d) Risk Implications
None

(e) Staffing Implications
None

(f) Property
None

(g) Equalities/Socio Economic Impact
None

(h) Climate Change and Biodiversity Impacts
None

(i) Consultations
The Depute Chief Executive (Education, Communities and Organisational Development), Head of Governance, Strategy and Performance, and, the Council's Information Assurance Group, as well as Estates and Property Services, Equalities, Head of Economic Growth and Development, Democratic Services Manager and Education Estates have all been consulted and their comments have been incorporated within the Policy.

6. CONCLUSION

6.1 The CCTV Policy is required to ensure Council wide consistent management of CCTV systems and the footage captured by these CCTV systems.

6.2 The Committee is asked to approve the attached CCTV Policy.

Author of Report: Alison Morris, Information Governance Manager & DPO
Background Papers: Appendix 1: CCTV (Closed Circuit Television) Policy
Ref: