EXECUTIVE MEMBER - THE MAYOR

Date: **Thursday 18th December, 2025**
Time: **10.00 am**
Venue: **Spencer Room (Municipal Buildings)**

AGENDA

1. Welcome and Fire Evacuation Procedure

   In the event the fire alarm sounds attendees will be advised to evacuate the building via the nearest fire exit and assemble at the Bottle of Notes opposite MIMA.

2. Apologies for Absence

   To receive any apologies for absence.

3. Declarations of Interest

   To receive any declarations of interest.

4. Announcements from the Mayor

   To receive any announcements from the Mayor.

5. Questions from Members of the Public (if any)

   To receive questions from members of the public.

6. Questions from elected Members (if any)

   To receive questions from elected Members.

THE MAYOR

7. Data Management Policy 2025-2028 3 - 18

   Report for decision.

8. Surveillance Policy 2026/7 19 - 56

Report for decision.

9. Artificial Intelligence Policy 57 - 72

Report for decision.

10. Any other urgent items which in the opinion of the Chair, may be considered.

Charlotte Benjamin
Director of Legal and Governance Services

Town Hall
Middlesbrough
Wednesday 10 December 2025

MEMBERSHIP

C Cooke - Elected Mayor

Assistance in accessing information

Should you have any queries on accessing the Agenda and associated information please contact Scott Bonner, 01642 729708, scott_bonner@middlesbrough.gov.uk

Agenda Item 7

MIDDLESBROUGH COUNCIL	Middlesbrough moving forward

Report of:	Charlotte Benjamin - Director of Legal and Governance Services
Relevant Executive Member:	Chris Cooke – The Mayor
Submitted to:	Single Member Executive – The Mayor
Date:	18 December 2025
Title:	Data Management Policy 2025 - 2028
Report for:	Decision
Status:	Public
Council Plan priority:	Delivering Best Value
Key decision:	No
Why:	Decision does not reach the threshold to be a key decision
Subject to call in?	Yes
Why:	Non-Urgent Report

Proposed decision(s)
That the Mayor: - **APPROVES** the Data Management Policy attached at Appendix 1.

Executive summary
The report seeks approval of the Data Management policy which has been reviewed in line with its scheduled triennial review to ensure the policy continues to be fit for purpose and aligns with the ambitions set out in the recently agreed Information Strategy. The Policy sets out the rules and guidance necessary to standardise, manage, link and exploit data throughout its lifecycle. The decision requires Single Member Executive approval as it is a 'minor variation to an existing policy or procedure' as per Section 10.21.2(a) of the constitution.

1. Purpose of this report and its contribution to the achievement of the Council Plan ambitions

1.1 This report presents and seeks approval of the proposed revisions to the Council's Data Management Policy following the scheduled triennial review in order to ensure our continued compliance with legislation. The policy sits within the Council's Information Governance Policy Framework.

1.2 The purpose of this policy is to implement a systematic approach to data management within the data lifecycle, and across the organisation, to support delivery of the Information Strategy that 'the right information will be available to the right users, at any time, accessible and used ethically to support achievement of the Council Plan.'

Our ambitions	Summary of how this report will support delivery of these ambitions and the underpinning aims
A successful and ambitious town **A healthy Place** **Safe and resilient communities**	Continued implementation and adherence to a Data Management Policy will ensure that the Council has a systematic approach to data management across the data lifecycle. Adherence to this policy will support the vision set out in the Council's Information Strategy that: 'the right information will be available to the right users, at any time, accessible and used ethically to support achievement of the Council Plan.'
Delivering best value	Successful adherence to the Policy will support robust and effective corporate governance by ensuring decisions made by the Council are based on sound data.

2. Recommendations

2.1 That the Mayor:

- **APPROVES** the Data Management Policy attached at Appendix 1.

3. Rationale for the recommended decision(s)

3.1 Reviewing the policy regularly is in line with good practice. It is recommended that the revised policy is agreed to ensure the Council has a policy framework against which it can continue to assess the quality of its data and take action to address poor quality data.

4. Background and relevant information

4.1. Key elements of the legislative and regulatory framework for data management are set out below. Failure to comply with this framework can lead to significant financial penalties, criminal prosecution and non-criminal enforcement action:

- UK General Data Protection Regulation 2016 (UK GDPR), Data Protection Act (DPA) 2018

- Data (Use and Access) Act 2025 (DUAA)
- Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended) (PECR)
- Digital Economy Act 2017
- Environmental Information Regulations 2004 (EIR)
- Freedom of Information Act (FOIA) 2000
- Local Government Acts 1972, 1985, 1988 and 1992
- Local Government Transparency Code 2015
- Lord Chancellor's Code of Practice on handling information requests
- And Other Regulations and Codes of Practice.

4.2. The policy sets out how the council should systematically manage its data across the data lifecycle to ensure the data that it holds is:

- accurate, complete, timely, relevant, reliable, valid and available
- standardised and linkable where possible
- explained where appropriate to ensure that it is not misused in error
- stored securely and in a manner that protects confidentiality and integrity
- securely disposed of in line with the Council's Retention Schedule.

5. Ward Member Engagement if relevant and appropriate

5.1 This is not applicable to this decision.

6. Other potential alternative(s) and why these have not been recommended

6.1 The Council could choose not to adopt corporate policies on data management, however statutory duties would remain in place and in the absence of a standard approach there would be an increased risk of making decisions that fail to meet those legal duties. Given these duties are in place this option is not recommended.

7. Impact(s) of the recommended decision(s)

Topic	Impact
Financial (including procurement and Social Value)	There are no direct costs associated with this report.
Legal	The policy supports the Council to be able to meet its various statutory duties in relation to the legislative and regulatory framework for data management listed above.
Risk	Approval of the policy will positively impact on risks within the Council's risk registers, primarily the risk that the Council fails to comply with the law.
Human Rights, Public Sector Equality Duty and Community Cohesion	There is no impact associated with the proposed policy within this area.
Reducing Poverty	There is no impact associated with the proposed policy within this area.

Climate Change / Environmental	There are no climate or environmental impacts associated with the proposed policy.
Children and Young People Cared for by the Authority and Care Leavers	There are no direct implications arising from this Policy on this group.
Data Protection	This policy will support compliance with Data Protection legislation.

Actions to be taken to implement the recommended decision(s)

Action	Responsible Officer	Deadline
Publication of the policy on the MBC Website and Intranet pages	V Holmes, Data and Analytics Manager	30 January 2026.

Appendices

1	Data Management Policy 2025 - 2028

Background papers

Body	Report title	Date
Executive	Information Strategy 2025 - 2029	8 October 2025

Contact: Victoria Holmes, Data and Analytics Manager
Email: Victoria_holmes@middlesbrough.gov.uk

Data Management Policy 2025 - 2028

Creator	Author(s)	Ann-Marie Johnstone (Head of Governance, Policy and Information); Victoria Holmes (Data & Analytics Manager).		
	Approved by	Leanne Hamer (Governance & Information Manager)		
	Department	Legal and Governance Services		
	Service area	Governance, Policy and Information		
	Head of Service	Ann-Marie Johnstone		
	Director	Charlotte Benjamin		
Date	Created	2022/09/23		
	Submitted	2025/10/15		
	Approved	TBD – planned for 20251218		
	Updating Frequency	3 years		
Status	Version: 2			
Contributor(s)	Head of Governance, Policy and Information and SIRO; Governance and Information Manager; Data Protection Officer; Data and Analytics Manager.			
Subject	Data management; statutory returns;			
Type	Policy			
	Vital Record		EIR	
Coverage	Middlesbrough Council			
Language	English			

Document Control

Version	Date	Revision History	Reviser
0.1	20190530	First draft	V Holmes
0.2	20190910	First revision	AM Johnstone
1.0	20191115	Finalised	P Stephens
1.1	20210316	Data classification approach added	L Hamer
1.2	20221130	Social Care Policy update	M Brearley
2.0	20251014	Second Draft Revision	V Holmes

Distribution List

Version	Date	Name/Service area	Action
1.0	20191130	WLMT	Implement
1.1	20210430	All staff via Intranet	Implement
1.2	20221130	All staff via Intranet	Implement
2.0	20260101	All staff via Intranet	Implement

Contact:	data@middlesbrough.gov.uk

Summary

This policy is part of the framework underpinning the Council's Information Strategy, and sets out how the Council will effectively standardise, manage, link and exploit data throughout its lifecycle, and ensure that it meets its obligations in respect of data integrity, statutory returns to Government, statutory information requests and data transparency.

The following sections outline:

- the purpose of this policy;
- definitions;
- scope;
- the legislative and regulatory framework;
- policy statement;
- roles and responsibilities;
- supporting policies, procedures and standards; and
- monitoring and review arrangements.

Purpose

The purpose of this policy is ensure a systematic approach to data management across the data lifecycle, across the organisation, to support the vision set out in the Information Strategy that 'the right information will be available to the right users, at any time, accessible and used ethically to support achievement of the Council Plan.'

This policy will ensure that the data it holds is:

- accurate, complete, timely, relevant, reliable, valid and available
- standardised and linkable where possible
- explained where appropriate to ensure that it is not misused in error
- stored securely and in a manner that protects confidentiality and integrity
- securely disposed of in line with the Council's Retention Schedule.

Compliance with this policy will deliver the following benefits:

- improved integrity, availability and sharing of data
- improved understanding of citizen and customer needs
- better and more timely decision-making and improved value for money
- ensuring good data quality will increase the Council's opportunities to automate processes through use of Artificial Intelligence. This can add value and improve outcomes
- ensure good data quality will support accurate forecasting through predictive analytics across Directorates.

It will also help the Council to mitigate the following risks:

- loss of data due to a lack of security
- data breach of sensitive information, either personal or commercial
- poor decision making or failure to act due to data shortcomings
- poor decision making due to poor data quality used in predictive analytics.

Definitions

Data management	The process for acquiring, validating, storing, protecting, and processing required data to ensure its security, confidentiality, integrity and availability for users and requesters.
Data integrity standard	The standard to which data sets will be maintained to ensure they meet required integrity standards (e.g. the level of completeness, accuracy, timeliness etc. required).
Data processing standard	The standard of processing to be maintained to ensure that data meets the integrity standard.
Digital continuity	The ability to access and maintain digital data throughout its lifecycle regardless of the system it is held on. Digital continuity should be ensured in the commissioning of a new system to avoid data loss or interruption through the extraction and migration of data the new system or an appropriate archiving solution.
Information	Refers to: (unstructured) data, (structured) information, and records (of interactions, policies or decisions). The Council holds information in many different formats; in physical and digital form, both online and offline; on premises and externally.
Golden record	A single, well-defined source of data for certain data points e.g. date of birth, address.
Records	Information created, received and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business.
Information security	Organisational and technical measures that are put in place to prevent security incidents that could affect the confidentiality, integrity, or availability of personal data.
Information classification	How the Council will classify information assets to ensure they are appropriately protected.
Data disposal	The process for ensuring data is securely disposed of and appropriately recorded once its retention period has passed.
Master Data Management	The method used to define and manage the critical data of an organisation to provide, via data integration, a single authoritative points of reference for e.g. customer, asset or spatial data.
Data anonymization	The process of rendering personal data anonymous in such a manner that the data subject is not or no longer identifiable.
Data pseudonymisation	The de-identification procedure by which personally identifiable information fields within a data record are replaced by one or more artificial identifiers, or pseudonyms.

Data lifecycle	Data lives through six stages – creation; organisation; access and use; maintenance; archiving and preservation and destruction. The life period of data is determined by the Council's Retention Schedule.
Personal data accuracy	Personal data should be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
Privacy by design	The legally required steps taken to integrate appropriate technical and organisational measures, from the design stage, to implement the data protection principles and safeguard individual rights with DPIAs being completed where necessary e.g. new purpose for existing data.
Smart data model	This standardised, interoperable data structures that define how real-world entities and concepts are digitally represented for consistent data sharing and integration.
Customer data	Data refers to any information relating to a customer's interactions with a trader, including details about supplied goods, services, or digital content, pricing, usage, and performance.
Business data	Data refers to any information about a trader's goods, services, or digital content, including details of their supply and customer feedback

Scope

This policy applies to all employees (both permanent and temporary), contractors and consultants of the Council who are given the authority to create, access, maintain or dispose of Council data.

It applies to all data created and /or maintained by the Council, whether created or received and managed directly, or by third parties on its behalf. It also applies to data created, received or managed by the Council in partnership with, or on behalf of, other organisations.

Legislative and regulatory framework

Key elements of the legislative and regulatory framework for data management are set out below. Failure to comply with this framework can lead to significant financial penalties, criminal prosecution and non-criminal enforcement action.

UK General Data Protection Regulation 2016 (UK GDPR), Data Protection Act (DPA) 2018	GDPR and the DPA places a duty on the Council to manage personal data in a way that complies with the data protection principles: lawfulness, fairness and transparency, purpose limitation, data minimisation,

	accuracy, storage limitation, integrity and confidentiality (security), and accountability. It also obliges the Council to respond to requests from individuals to exercise their data protection rights where these apply including the rights: to be informed, of access, to rectification, to erasure, to restrict processing, to data portability, to object, or relating to automated decision-making and profiling.
Data (Use and Access) Act 2025 (DUAA)	Updates some areas of data protection law and adds new functions including Digital Verification Services, National Underground Asset Register, Digitising Registers of Births and Deaths, and Online Data Processing.
Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended) (PECR)	PECR regulates the privacy rights of individuals relating to electronic communications including: marketing calls, emails, texts and faxes; cookies (and similar technologies); keeping communications services secure; and customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings.
Digital Economy Act 2017	Provides government powers to share personal information across organisational boundaries to improve public services.
Environmental Information Regulations 2004 (EIR)	Deriving from European law, this provides for public access to 'environmental information' held by public authorities, unless specific exception(s) apply. It is also obliged to proactively and routinely publish information that has been frequently requested in the past in its Publication Scheme.
Freedom of Information Act (FOIA) 2000	Under the FOIA, the Council has a duty to make information available to the public upon request, unless specific exemption(s) apply. It is also obliged to proactively and routinely publish information that has been frequently requested in the past in its Publication Scheme. Poor data quality would hinder the amount of information the Council could publish.
Local Government Acts 1972, 1985, 1988 and 1992	Establishes requirements to manage records and information, and requires councils to use data to make informed decisions to ensure value for money and compliance with a range of statutory duties.
Local Government Transparency Code 2015	Requires local authorities to publish certain information, specifying content and frequency of publication, and recommends the publication of certain other information.
Lord Chancellor's Code of Practice on handling information requests	Issued under s.45 of the FOIA, the code sets out the practices which public authorities should follow when dealing with requests for information under the Act.

Other Regulations and Codes of Practice	The Council's approach is also informed by range of other regulations and codes of practice, including: • ISO 15489 Records Management; • Lord Chancellor's Code of Practice on the management of records; • National Data Guardian's Data Security Standards; • Requirements for statutory data returns to Government departments; • Re-use of Public Sector Information Regulations 2005; • 'Caldicott principles' on NHS patient information (revised 2013) and the NHS Data and Protection Toolkit; • National Data Opt-Out in Health and Social Care • ONS Code of Practice for statistics (voluntary application); • Open Standards Principles; and • Information Commissioner's Office (ICO) Data Sharing Code of Practice (forthcoming). • ICO Anonymisation Guidance

Policy detail

The Data and Analytics Team will work collaboratively with Information Asset Owners, Information System Owners and other key personnel to optimise the performance of its data, ensuring that it is of the appropriate quality and integrity, is easily accessible and works smoothly.

This work will ensure that the Council's datasets are of the right standard support evidence-based approaches to strategy, policy and commissioning and so effectively support the delivery of its strategic objectives. Data gaps identified by this work will be progressed in line with the Council's priorities.

Data will be developed in standardised and linkable formats (e.g. 5-star Open Data) to support transparency and reuse. Where appropriate, each data item (e.g. case files) will be allocated a core Unique Reference Number (URN), where possible standardised national numbers such as National Insurance or NHS numbers to support the development of golden records, master data management and ultimately improved intelligence.

Business Intelligence dashboards will be made available for all services, and routinely used to manage service performance, drive data improvements, forecast future events via Predictive Analytics utilising Predictive Analytics Standard including Python Code and drive day-to-day decision-making. These automated data products rely on accurate data and therefore data quality will be a core consideration when developing future data products.

Equality and Inclusion must meet our data quality standards as inaccurate data can result in unfair actions and outcomes for individuals. Adherence to this policy will support the

Council to be able to implement innovative, automated uses for data that will be heavily reliant on data being timely and accurate in order to be able to automate its use effectively.

In order to support Business Continuity, the Data & Analytics team will scope (in conjunction with Service areas) data extracts that will enable continuation of operational duties in the event of cyber outage.

The Council will develop and implement solutions to support the digitisation and integration of all appropriate datasets, implementation of master data management, data harvesting and data archiving.

Source data will be held securely, with extra security measures in place for personal data. Where data is required to be analysed or shared in a raw format for internal and external parties, a privacy by design approach will be taken with data provided in anonymised or pseudonymised form.

Personal data will only be provided in fully identifiable form where this complies with data protection principles and rights. Appropriate records will be maintained of personal data shared with other agencies.

Within the legal and regulatory framework set out below, the Council will develop a 'by default' and, where possible, automated approach to data sharing with our partners and contractors, to support collaborative planning, commissioning and service design.

The Council's Data Protection Officer will provide advice and guidance on all such matters as required.

Roles and responsibilities

Effective records management is the collective responsibility of all those individuals named within the scope of this policy.

Senior Information Risk Owner (SIRO)	Responsible for the overall management of information risk within the Council, advising the Chief Executive, management team and Information Asset Owners, and ensuring that staff training is available and fit-for-purpose. The role is undertaken by the Head of Governance, Policy and Information, who is also responsible for the Information Strategy. Responsible for ensuring that data integrity and availability issues are raised with Information Asset Owners and System Owners to address.
Data & Analytics Manager	Responsible for the development and implementation of the Council's data management policy and supporting procedures, to ensure that the Council meets its obligations in respect of data integrity, statutory returns to the Government and data transparency. This policy gives the Data Manager a mandate to drive work necessary to comply with the standards set in this policy

	which are necessary to deliver the ambitions of the Information Strategy. Also, a key user of products from the Data Team. Responsible for ensuring that data used within business intelligence products complies with the standards required by this policy. Responsible for the delivery of predictive analytics products, to enable it to accurately predict future service demand to improve service planning and inform its preventative services, which will be designed to reduce demand for more intensive interventions by supporting people at an earlier stage. To facilitate Business Continuity across the council, by providing data extracts to support service areas during cyber outage.
Records Manager	Responsible for the development and implementation of the Records Management policy and supporting procedures, which will complement this policy. Providing advice and checking compliance to ensure the Council's records and well-kept and that the systems used to hold them are fit-for-purpose. The Records Manager owns the ECMS and mail and print contracts and is responsible for inactive records where an information asset owner cannot be identified.
Data Protection Officer	Responsible for assisting the council to monitor internal compliance, informing and advising on data protection obligations, providing advice regarding Data Protection Impact Assessments (DPIAs), and acting as a contact point for data subjects and the supervisory authority.
Information System Owner	All information systems within the Council have an assigned owner. System owners are responsible for the security, confidentiality, integrity of availability of the information within the system and work alongside ICT, Information Asset Owners and Information Asset Assistants to implement appropriate processes and procedures to ensure agreed standards are achieved and maintained.
Information Asset Owner	Responsible for maintaining comprehensive and accurate information asset registers (IARs) for their service areas, and ensuring that: • staff in their service area are aware of their responsibilities and appropriately trained; • data and records are managed in line with the Council's policy and procedures; • information is released in line with legal requirements and this policy; and • identifying and escalating information risks to the SIRO.

Information Asset Administrators	Information Asset Administrators (IAAs) support IAOs in the good governance of information and managing information risks. IAAs will include all managers and supervisory staff and other staff with specific roles relating to the security, confidentiality, integrity and / or availability of information.
Senior System users	Senior system users ('super users') support the Information System Owner and, working with frontline users, are responsible for ensuring data is managed in line with this policy and supporting procedures.
All managers	Responsible for overseeing day-to-day compliance with this policy by their staff and other personnel they manage.
All staff, contractors, consultants, interns and any other interim or third parties	Responsible for creating, accessing, using and managing data and intelligence in accordance with this policy and its supporting procedures.
Information Strategy Group	Operational group of key officers led by the SIRO responsible for implementing the Information Strategy, in conjunction with Information Asset Owners.
Risk Management Group	The group ensures the Council has a suitable risk management framework in place, provides a mechanism for risk management issues to be discussed and ensures the delivery of the Risk Improvement Plan

Supporting policies, procedures and standards

The following policies, procedures and standards will be implemented across the Council to ensure that the Council's data is managed effectively.

Data standardisation framework	Outlines procedures to enable the Council to standardise datasets and allow data to be effectively utilised, including data minimization.
Data Protection Policy	Sets out how the Council complies with data protection legislation.
Digital Communications Policy	This policy is part of the framework underpinning the Council's Information Strategy, and sets out how the Council will ensure that its 365 email system is operated in line with the principles of effective information governance. It also places email usage within the context of the Council's Digital Strategy.
ECMS procedures	Sets out business rules in respect of the use of the Council's Enterprise Content Management System as the proper tool for the storage and referencing of digital records.
Public Information and Information Requests Policy	This establishes the corporate framework for responding to statutory information requests, and to proactively identify information to be routinely published using Open Standards and

	to meet the Council's requirements under the transparency code.
Records Management Policy	Sets out how the Council will manage its records to ensure they are digitized where appropriate, held securely and deleted when retention periods are reached.
Records Retention Schedule	This defines how long different records should be retained to comply with legal, regulatory or other requirements and the proper arrangements for archiving and destruction.
Sensitivity Labels	This guidance covers the rules when applying sensitivity labels to your content and applies across OneDrive, SharePoint and email. By applying sensitivity labels to this content it ensures that we keep our information secure by stating how sensitive certain information is within MBC.
Vital Records Standards	This sets out how vital records will be identified and the steps to be taken to ensure their protection and preservation.
Business Continuity Plans	These identify those vital records required to support delivery of critical services.
Disaster Recovery Plan	This identifies priorities and recovery timescales for access to ICT systems and digital records in the context of business continuity.
Predictive Analytics Standard	This document sets out the essential factors and critical information to consider when developing predictive analytics (including Python Code of Conduct) that supports strategic decision-making
AI Policy (in development)	Development of AI Policy is underway which will sets out Middlesbrough Council's framework for the lawful, ethical, and effective use of AI to improve productivity, protect personal data, and assure residents, staff, and businesses that AI is used responsibly and safely as part of its Information Governance and Digital Strategy.

Monitoring and review arrangements

The implementation and effectiveness of this policy and its supporting procedures will be overseen by the Information Strategy group which is delivering the detailed delivery plan for the strategy. That plan includes actions to improve data quality.

This policy will be reviewed every three years, unless there is significant development that would require a more urgent review e.g. new legislation.

This page is intentionally left blank

MIDDLESBROUGH COUNCIL	Middlesbrough moving forward

Report of:	Charlotte Benjamin - Director of Legal and Governance Services
Relevant Executive Member:	Chris Cooke - The Mayor
Submitted to:	Single Member Executive – The Mayor
Date:	18 December 2025
Title:	Surveillance Policy 2025-6
Report for:	Decision
Status:	Public
Council Plan priority:	Delivering Best Value
Key decision:	No
Why:	Decision does not reach the threshold to be a key decision
Subject to call in?	Yes
Why:	Non-Urgent Report

Proposed decision(s)
That the Mayor: - **APPROVES** the Surveillance Policy 2025-26 - **NOTES** the content of this report on use of surveillance powers in 2025.

Executive summary
This report seeks approval of the Surveillance Policy 2025-6. In accordance with the Statutory Codes of Practice applying to the Regulation of Investigatory Powers Act 2000 (RIPA), the Council is required to review its use and set out the Policy at least annually.

1. Purpose of this report and its contribution to the achievement of the Council Plan ambitions

1.1 This report seeks approval of the proposed Surveillance Policy 2025-26.

1.2 Guidance underpinning the Regulation of Investigatory Powers Act (RIPA) 2000 states that elected members should review the Council's use of RIPA powers and set the RIPA policy annually.

1.3 Use of RIPA powers are considered annually by Audit Committee as part of the annual report of the Senior Information Risk Owner. Statistical information on use of the powers is also regularly reported to the relevant Scrutiny Panel.

Our ambitions	Summary of how this report will support delivery of these ambitions and the underpinning aims
A successful and ambitious town **A healthy Place**	Implementation and adherence to a Surveillance Policy does not directly impact on these ambitions, however compliance with the principles of the policy will ensure the Council adheres to the law, its obligations and duties imposed on it under legislation.
Safe and resilient communities	Compliance with the policy will ensure that the Council acts lawfully when conducting activities that fall within the scope of the policy. It safeguards privacy by minimising intrusion and proportionally applies necessity tests before surveillance is authorised. It will ensure that the Council protects communities in the following areas: • Crime prevention and public safety • Safeguarding vulnerable groups • Accountability and trust • Protecting privacy • Community reassurance.
Delivering best value	Effective compliance with the policy ensures resources are used effectively and responsibly while achieving community safety goals. It: • Provides a strict framework for use of surveillance preventing unnecessary deployment. • Adheres to Data Protection, Human Rights, and RIPA laws. Reducing the risk of fines, legal challenge or reputable damage. • Provides evidence-based decision making supporting targeted interventions. • Provides transparency that builds public trust. • Supports partnership working with police and other agencies.

2. Recommendations

2.1 That the Mayor:

- **APPROVES** the Surveillance Policy 2025-26
- **NOTES** the content of this report on use of surveillance powers in 2025.

3. Rationale for the recommended decision(s)

3.1 The proposed policy will ensure that surveillance activity undertaken by the Council complies with its strategic priorities and statutory obligations, is lawful and that due regard is given to human rights and to data protection rights. A decision from the Mayor is sought as the agenda item is within their portfolio.

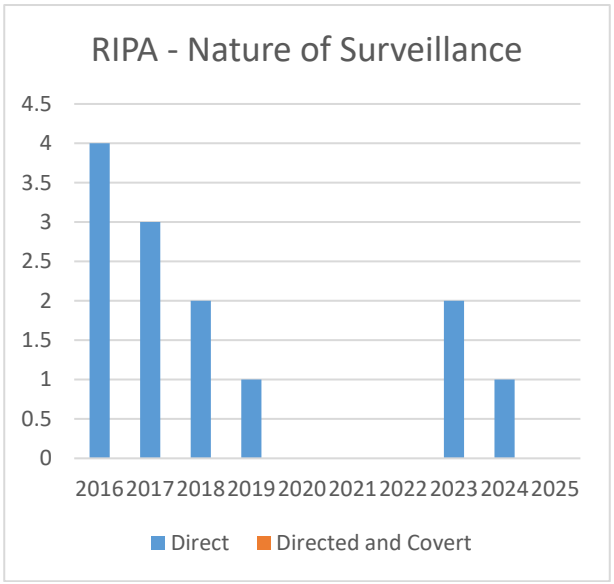
4. Background and relevant information

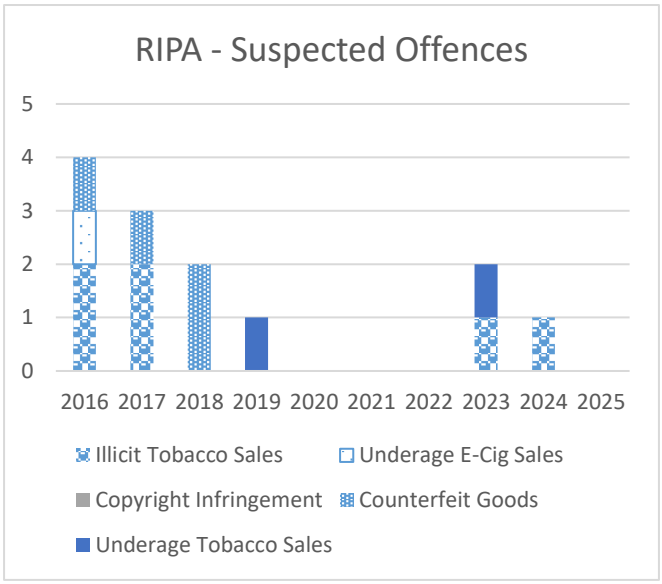
Use of RIPA

4.1 RIPA is the law governing the use of surveillance techniques by public authorities, including local authorities. RIPA covert surveillance powers can only be used if surveillance is necessary, proportionate, and compatible with human rights and where the Council is the prosecuting authority. There are also further restrictions which mean RIPA can only be used where there could be a custodial sentence of six months or more, or where surveillance relates to the sale, allowing the sale and or persistently selling alcohol to children as well as the sale of tobacco to persons under 18 years old.

4.2 In such instances, covert surveillance can be undertaken, subject to magistrate approval, if it is not possible to gather sufficient evidence to secure a prosecution without this.

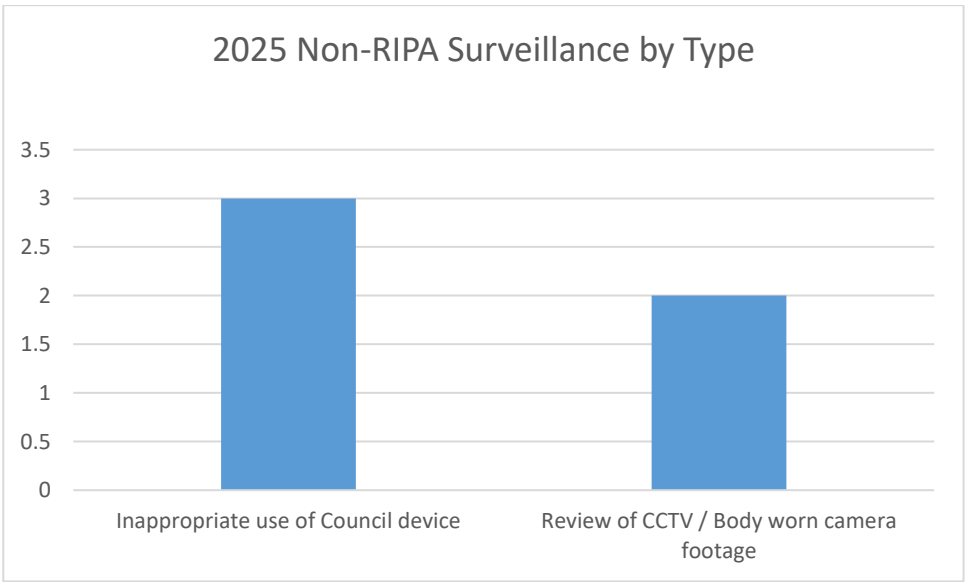
4.3 The charts below set out the past ten years of RIPA activity undertaken by the Council, the nature of the surveillance and the reasons why it was undertaken. To note, the Council always looks to methods to gather information that do not require covert surveillance to be undertaken, in order to minimise use of this power, therefore activity remains low. There were no applications to use covert surveillance under RIPA in 2025.





Non-RIPA surveillance

4.4 The Council also has in place a process, set out within the Surveillance policy, which governs the application of requests for surveillance on non-RIPA grounds. The data for 2025 relates to staffing matters, these are centrally logged and approved by the HR manager to again ensure the use of this power is minimised and that a legitimate basis for use is identified prior to approval. The table below sets out the reasons this power used to investigate the following potential issues:



Monitoring and review

4.5 This Policy is updated annually and was last approved by the Mayor in December 2024.

4.6 The Council continues to maintain an overarching Surveillance Policy (Appendix 1), which covers CCTV, RIPA, non-RIPA covert surveillance and the surveillance of employees.

4.7 The Council's policy aligns with guidance published by the Information Commissioners Office on monitoring workers.

4.8 The Surveillance policy review this year has had minor amendments to reflect staffing changes, no other change has been necessary. The policy is supported by corporate e-learning.

5. Ward Member Engagement if relevant and appropriate

5.1 Not applicable.

6. Other potential alternative(s) and why these have not been recommended

6.1 The Council should have a policy that sets out how it complies with RIPA. It could choose not to have a policy that covers both RIPA and non-RIPA activity. However, this is not recommended, as a single policy provides for a coherent and systematic approach and is in line with the Council's commitment to openness and transparency.

Impact(s) of the recommended decision(s)

Topic	Impact
Financial (including procurement and Social Value)	It is anticipated that all activities require by the policy are achievable within existing and planned budgets.
Legal	The report and its associated action plan, demonstrates how the Council does and will continue to meet its various legal duties when undertaking surveillance.
Risk	Implementation of the proposed Surveillance Policy mitigates a number of risks within the Council's strategic and information risk registers, having a positive overall impact on the strategic risk that the Council could fail to comply with the law.
Human Rights, Public Sector Equality Duty and Community Cohesion	The proposed policy has been subject to Level 1 (screening) equality impact assessment (at Appendix 2). This assessment identified that no negative differential impacts on diverse groups and communities within Middlesbrough is anticipated from the implementation of the policy.
Reducing Poverty	The policy is not directly relevant to this commitment.
Climate Change / Environmental	There are no climate or environmental impacts associated with the proposed policy.

Children and Young People Cared for by the Authority and Care Leavers	There are no direct implications arising from this Policy on this group as identified in the equality impact assessment (Appendix 2).
Data Protection	This policy aims to balance the business interests of the Council as an employer and workers' rights and freedoms under data protection law. It is imperative that the Council has an up-to-date policy which advises staff on proper use of these powers to ensure any action is lawful, necessary and proportionate.

Actions to be taken to implement the recommended decision(s)

Action	Responsible Officer	Deadline
Publication of surveillance policy on the MBC Website and Intranet pages	L Hamer, Governance and Information Manager	5 January 2026

Appendices

1	Surveillance Policy 2025 - 2026
2	Surveillance Policy 2025 - 26 – Impact Assessment Level 1: Initial screening Assessment

Background papers

Body	Report title	Date
Corporate Affairs and Audit Committee	Annual Report of the Senior Information Risk Owner (SIRO)	31 March 2022
Corporate Affairs and Audit Committee	Annual Report of the Senior Information Risk Owner (SIRO)	April 2023
Executive Member for Finance and Governance	Surveillance Policy	20 December 2023
The Mayor	Surveillance Policy	17 December 2024

Contact: Ann-Marie Johnstone, Head of Governance, Policy and Information
Email: ann-marie_johnnstone@middlesbrough.gov.uk

Surveillance Policy

Creator	Author(s)	Ann-Marie Johnstone Leanne Hamer			
	Approved by	Executive Member			
	Department	Legal and Governance Services			
	Service area	Policy, Governance and Information			
	Head of Service	Ann-Marie Johnstone			
	Director	Charlotte Benjamin			
Date	Created	20251111			
	Submitted	20251218			
	Approved	TBC			
	Updating Frequency	Annually, unless review triggers met in interim			
Status	Version: 10.0				
Contributor(s)	Governance and Information Manager; Data Protection Officer, HR Manager, Operational Community Safety Manager				
Subject	Overt and covert surveillance				
Type	Policy				
	Vital Record		EIR		
Coverage	Middlesbrough Council				
Language	English				

Document Control

Version	Date	Revision History	Reviser
8.0	2023/11	Review	L Hamer
9.0	2024/11	Review	AM Johnstone
10.0	2025/11	Review	L Hamer

Distribution List

Version	Date	Name/Service area	Action
7.0	2022/12	All stakeholders	Note
8.0	2023/11	All stakeholders	Note
9.0	2024/11	All stakeholders	Note
10.0	2025/12	All Stakeholders	Note

Contact:	data@middlesbrough.gov.uk

Summary

1. This policy provides a framework for the undertaking of surveillance by the Council of the public and of its employees, where appropriate, ensuring that any surveillance undertaken is lawful and that due regard is given to human rights and to data protection rights.

2. The following sections outline:

    - the purpose of this policy;
    - definitions;
    - scope;
    - the legislative and regulatory framework;
    - roles and responsibilities;
    - policy detail;
    - supporting policies, procedures and standards; and
    - monitoring and review arrangements.

Context

3. This Policy links to HR related policies as surveillance involves monitoring employees and handling personal data. These connections include:

    - Data Protection Policy,
        i. Collection of personal data (e.g. CCTV footage)
    - Wider IT Security Policies
        i. If surveillance includes monitoring emails, internet usage or devices, this links to ICT policies
    - Disciplinary Policy
        i. Ensuring fairness and transparency in disciplinary processes
    - Health & Safety Policy
        i. CCTV or monitoring used for safety purposes , assurance this aligns with duty of care obligations
    - Equality & Inclusion Policy
        i. Not discriminating or disproportionately targeting certain groups
        ii. Checks on compliance with equality legislation

Purpose

4. This policy provides a framework for undertaking surveillance activities in compliance with all applicable laws by:

    - creating and maintaining organisational awareness of the right to respect for private and family life (Article 8, Human Rights Act 1998) as an integral part of operations;
    - ensuring that all employees are aware of and fully comply with the relevant legislation as described in this policy and fully understand their own responsibilities when planning and undertaking surveillance activities;

- where necessary, ensuring that all employees obtain the appropriate authorisations when undertaking surveillance activities; and
- ensuring that sensitive and confidential surveillance information is stored, archived and disposed of in an appropriate manner.

Definitions

5. Appendix 1 defines the key terms used in this policy. Where appropriate, the definitions used by the Council are aligned with those in legislation or supporting codes of practice.

Scope

6. The policy applies to all overt and covert surveillance undertaken by or on behalf of the Council. This includes, but is not limited to the following:

    - the taking of photographs of someone in a public place;
    - the recording by video cameras of someone in a public place;
    - the use of listening devices or photographic equipment to obtain information in respect of activities in a residential premises or private vehicle;
    - the acquisition of communications data from third party service providers;
    - the viewing of someone's social media activity;
    - the taking of photographs of employees in the workplace;
    - the recording by video cameras of employees in the workplace;
    - the viewing of an employee's social media activity; and
    - the acquisition of employees' communication data or other tracking data during the course of work.

7. Currently the Council does not use drones for surveillance or enforcement purposes.

8. The policy applies to all Council employees and any other party undertaking surveillance on behalf of the Council by contract. Non-compliance with this policy may result in disciplinary action, other sanction for employees or for other parties enforcement in relation to the terms and conditions of the contract.

9. This policy is approved, and its application scrutinised by elected members but members will have no direct involvement in surveillance operations or in making decisions on specific authorisations.

10. The policy does not apply to householders or businesses who have obtained grants from the Council for the purpose of installing domestic or commercial CCTV. Equipment paid for and installed under these grants is not the property of the Council and the Council has no legal responsibilities for such equipment, or the information obtained by its use

Legislative and regulatory framework

11. The Council must comply with all relevant applicable legislation pertaining to surveillance, as outlined below

Human Rights Act 1998

12. The Human Rights Act 1998 (HRA) gave effect in UK law to the rights set out in the European Convention on Human Rights (EHCR).

13. The HRA requires that all action which may potentially impact on an individual's human rights is proportionate, necessary, non-discriminatory and lawful. The HRA lists sixteen basic human rights, which are either absolute, limited or qualified. All activity undertaken by the Council must comply with the HRA, including surveillance.

14. Article 8 of the EHCR – the qualified right to respect for private and family life, home and correspondence – is most likely to be engaged when local authorities seek to obtain private information about a person by means of surveillance. Covert surveillance, in particular via RIPA, are likely to engage the limited right to a fair and public hearing (Article 6).

Regulation of Investigatory Powers Act 2000

15. Part II of the Regulation of Investigatory Powers Act 2000 (RIPA) does not grant powers to undertake surveillance but does provide a statutory framework under which appropriate covert surveillance activity undertaken by local authorities (specifically directed surveillance and the use of CHIS) can be authorised, conducted and supervised compatibly with Article 8 of the EHCR and the Data Protection Act 2018.

16. RIPA aims to balance the rights and freedoms of individuals with the need for law enforcement and security agencies to have powers to perform their roles effectively.

17. The grounds on which local authorities can rely to authorise directed surveillance are narrower than those available to security services or the police. A local authority can only authorise directed surveillance of a member of the public if the designated person believes that such surveillance is necessary and proportionate for the purpose of preventing or detecting a crime which the local authority has legal powers to prosecute. In most cases the threshold is an offence for which there is a minimum prison sentence of six months, and the surveillance must also be authorised by a magistrate.

18. The acquisition of a RIPA authorisation will equip the Council with the legal protection (the RIPA 'Shield') against accusations of a breach of Article 8. Failure to comply with RIPA does not necessarily mean that surveillance would be unlawful, however it does mean that evidence obtained from surveillance could be inadmissible in court proceedings and so jeopardise a successful outcome.

Unauthorised action could also be open to challenge as a breach of the HRA and a successful claim for damages could be made against the Council.

19. Appendices 3 to 6 set out the forms that must be completed when applying for authority to conduct directed surveillance using RIPA, renewing authorisation and cancelling directed surveillance. Appendices 7 to 10 set out the same process for use of Covert Human Intelligence Sources using the RIPA legal framework.

20. A number of Codes of Practice have been issued under Part II of RIPA, as listed below. This policy and its supporting procedures fully comply with these codes.
    Interception of communications: code of practice 2016
    Equipment interference: code of practice
    Codes of practice for the acquisition, disclosure and retention of communications data
    Covert surveillance and covert human intelligence sources codes of practice
    Code of practice for investigation of protected electronic information
    Employment practices and data protection: monitoring workers | ICO

Data Protection Act 2018

21. Middlesbrough Council is a 'competent authority' for the purposes of Part 3 of the Data Protection Act 2018 (DPA) where it has authority or powers to investigate and prosecute criminal offences.

22. In this role the Council will comply with the law enforcement principles, which are reflected within this policy as appropriate. Processing of personal data for any of the law enforcement purposes must be:

    - lawful and fair;
    - collected and only processed for a specified, explicit and legitimate purpose;
    - adequate, relevant and not excessive;
    - accurate and, where necessary, kept up to date, and that personal data that is inaccurate is erased or rectified without delay;
    - kept for no longer than is necessary and storage periodically reviewed; and
    - processed in a manner that ensures appropriate security.

23. All other personal data that is not processed for law enforcement purposes falls under the UK General Data Protection Regulation 2016 (UK GDPR) and other applicable Parts of the DPA including appropriate exemptions (referred to as 'the data protection legislation'). In this general processing role, as a data controller, the Council will comply with the GDPR principles, which are reflected in this policy as appropriate.

24. Personal data will be:

    - processed lawfully, fairly and in a transparent manner;
    - collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, kept up to date;
- kept in a form which permits identification of data subjects for no longer than is necessary; and
- processed in a manner that ensures appropriate security of the personal data.

25. As a data controller, the Council will be responsible for and be able to demonstrate compliance with these principles.

Protection of Freedoms Act 2012

26. The Protection of Freedoms Act 2012 (POFA) provides for a wide range of measures to protect and promote the freedoms of individuals. Part 2 of the POFA required a new Code of Practice on surveillance technologies and the appointment of a Surveillance Camera Commissioner to oversee and review the operation of the Code.

27. A Surveillance Camera Code of Practice was published in 2013 and provides guidance on the appropriate and effective use of surveillance camera systems by relevant authorities and sets out 12 guiding principles that should be adopted by systems operators:

    - Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
    - The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
    - There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
    - There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
    - Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.
    - No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.
    - Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.

- Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
- Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
- There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.
- When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.
- Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

28. POFA also amends s28 of RIPA and brought in the requirement for a magistrate to approve a RIPA authorisation when the crime threshold is met. The threshold is a criminal offence which attract a minimum custodial sentence of six months or more. There are some limited exceptions to the six month rule, specifically:

    - the sale of alcohol to children (S.146 of the Licensing Act 2003);
    - allowing the sale of alcohol to children (S.147 of the Licensing Act 2003);
    - persistently selling alcohol to children (S.147A of the Licensing Act 2003); and
    - the sale of tobacco to persons under 18 years of age (S.7 Children and Young Persons Act 1933).

Investigatory Powers Act 2016

29. The Investigatory Powers Act 2016 (IPA) commenced on 11 June 2019 and is now the main legislation governing local authorities' access to communications data in order to carry out their statutory functions as a 'competent authority' under the DPA, replacing the framework set out in RIPA.

30. The Communications Data Code of Practice sets out the process for acquiring communications data in line with the Act.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

31. These regulations implemented Article 5 of the EU Telecoms Privacy Directive and gave businesses the right to intercept communications on their own networks, which occur as part of lawful business practice, and for the certain purposes.

32. Interception is lawful for the purposes of monitoring or recording, if doing so:

- allows the business to comply with other regulations;
- establishes the existence of facts;
- acts as a means of verification that the person being monitored is performing his or her work to standards;
- is in the interests of UK security;
- may prevent or detect criminal activity;
- ensures the communication system operates effectively; and
- allows the business to detect unauthorised use of the system.

Employment Practices Code

33. The Information Commissioner's Office's Employment Practices Code provides a framework under which surveillance of the activity of employees can be authorised and conducted compatibly with Article 8 of the HRA and the DPA. It covers amongst other matters, how employees can be monitored in the workplace and their right to work in a comfortable environment. Monitoring of employees should only take place where there is a real risk to the business and in line with the DPA, employees should be told about monitoring practices and under what circumstances their communications might be intercepted. A form that must be completed for the authorisations is in place and available on the Council's intranet page. Authorisations must be approved by the HR Manager

Policy detail

34. The Council will use overt and covert surveillance within its operations where it is appropriate to do so.

Overt surveillance

35. Most of the surveillance carried out by the Council will be done overtly e.g. general observations made by officers in line with their job roles and legal powers.

36. Overt surveillance using relevant equipment will be undertaken in line with the national Surveillance Camera Code of Practice. The Council will maintain a local code of practice that fully complies with the national code and keep this up to date.

37. The SRO will appoint a SPoC for CCTV and notify the Surveillance Camera Commissioner accordingly.

38. The SPoC will oversee all CCTV schemes operated by or on behalf of the Council and ensure their compliance with the national and local codes.

39. Scheme managers and responsible officers will be identified for all schemes and they will maintain Code Assessment Packs, demonstrating compliance with the Council's local code of practice.

40. Scheme managers will ensure that DPIAs are undertaken before any surveillance system is installed, whenever new technology or functionality is

being added onto or removed from an existing system, or whenever there are plans to process more sensitive data or capture images from a different location.

41. Scheme managers will ensure that responsible officers and surveillance camera operators working within their schemes are trained to the standard required by the Council's Code of Practice and have signed appropriate confidentiality agreements.

42. The SPoC will produce an annual report based on a review of annual self-assessments from scheme managers. The annual report will cover all schemes and equipment operated by the Council, covering:

    - operating arrangements, including contracts;
    - performance of schemes;
    - compliments and complaints received;
    - outcome of any inspections or audits in the year;
    - assurance the scheme continues to operate in compliance with legislation and relevant codes of practice; and
    - whether the scheme and / or individual cameras are still required.

43. From time to time, the Council may offer grants to residents for the installation of domestic CCTV systems. Equipment paid for and installed under these grants is not the property of the Council and the Council has no legal responsibilities for such equipment.

44. Outside of contractual arrangements, the Council will not direct any third party to undertake surveillance on its behalf. Any footage provided to the Council as potential evidence of criminality will only be processed where the Council has a lawful basis to do so and where the footage has been captured in line with data protection legislation.

Overt use of recording – virtual meetings

45. From time to time, officers within the Council may identify a legitimate need to record an online interaction using the Council's meeting software tools, or those of any Council supplier, excluding the streaming and recording of formal member committee meetings which are open to the public. Any officer wishing to do this must first assure themselves that recording the interaction is necessary and proportionate to the purpose identified having sought advice from the Data Protection Officer and prior approval from the Senior Information Risk Owner. There is a process in place to govern when formal committee meetings of the Council will be recorded.

Covert surveillance

46. The Council will use covert surveillance to acquire information to support investigations where it is lawful and appropriate to do so.

47. Covert surveillance will only be used where it is not considered possible to obtain the necessary information to progress investigations by overt means e.g.

interview. In addition, the method of surveillance must be proportionate and the least harmful means of gathering the information.

48. Covert surveillance does not require authorisation when it is in immediate response to events and it is not reasonably practicable for authorisation to be sought e.g. CCTV tracking of a crime in progress to assist police detection of offenders. When covert surveillance has been used in such circumstances it will be noted in the incident report(s) of the employee(s) that have undertaken the surveillance.

49. In the majority of circumstances, however, covert surveillance will be directed, planned, and authorised, through either (i) the framework provided by the Regulation of Investigatory Powers Act 2000, or (ii) internal authorisation processes that follows the spirit and principles of RIPA to ensure that such covert surveillance is necessary, proportionate, non-discriminatory, uses suitable equipment, and is lawful. This is set out in the supporting forms at appendices 3 to 6.

50. The Council will carry out covert surveillance to progress investigations outside of the RIPA framework, where (i) while significant, the matters under investigation may not typically result in criminal proceedings, or (ii) the potential criminal offence(s) under investigation are likely to attract a penalty below the RIPA threshold. Examples of such instances include but are not limited to:

    - suspected benefit fraud;
    - children at risk as court orders are not being respected;
    - serious cases of anti-social behaviour; or
    - contractors failing to carry out contracted works.

51. Both RIPA and non-RIPA surveillance will use a systematic process of:

    - application;
    - authorisation;
    - conduct of authorisation;
    - review;
    - renewal (where necessary); and
    - cancellation.

52. The following standard forms for RIPA applications will be used and provided via the Coordinating Officer (Auditor). Forms for internal authorisation of non-RIPA covert surveillance are also in place.

    - Application for use of directed surveillance
    - Review of use of directed surveillance
    - Renewal form for directed surveillance
    - Cancellation of use of directed surveillance form
    - Application for the use of covert human intelligence sources (CHIS)
    - Reviewing the use of covert human intelligence sources (CHIS)
    - Renewal of authorisation to use covert human intelligence sources (CHIS)

- Cancellation of covert human intelligence sources (CHIS)

Application

53. Only officers that can reasonably be expected to undertake covert surveillance as part of their job description will plan and apply for the authorisation of such surveillance.

54. At the start of an investigation, the applicant will consider whether the alleged activity proposed for surveillance is a potential criminal offence that meets the RIPA threshold, as defined within this policy.

55. If this threshold is met, the applicant will complete the mandatory RIPA application form (directed surveillance and / or CHIS). If the threshold is not met, then the applicant will complete and submit the Council's non-RIPA application form.

56. Both forms provide for consideration of necessity and proportionality and the likelihood of collateral intrusion and gathering confidential information, and how this can be mitigated. In completing the form(s), the applicant will have regard to the relevant code(s) of practice, the Council's covert surveillance procedure and associated guidance, and be advised by the SRO, Coordinating Officer (Auditor) and / or Legal Services where required.

57. The applicant considers the surveillance to be justified following completion of the forms, then a URN should be obtained from the Coordinating Officer (Auditor) and the form submitted to an appropriate authorising officer as defined by this policy for authorisation.

Authorisation

58. Authorisation is an appropriate safeguard against the abuse of power by public authorities. The appropriate authorising officer will assess the request for authorisation applying the same tests and the applicant, ensuring that a defensible case can be made for the conduct to be authorised.

59. In completing the form(s), the authorising officer will have regard to the relevant code(s) of practice, the Council's covert surveillance procedure and associated guidance, and be advised by the SRO, Coordinating Officer (Auditor) and / or Legal Services where required.

60. Having taken these issues into account, the authorising officer will either approve, part-approve or reject the application, updating the form(s) in writing. The authorising officer cannot add activity that they may wish to see on to the application.

61. The authorising officer will notify the applicant and the Coordinating Officer (Auditor) of the decision reached.

62. Before an authorisation can take effect it must be approved by a Justice of the Peace (a District Judge or Magistrate) in the case of RIPA applications, or the SRO, in the case of non-RIPA applications. The Coordinating Officer will liaise with the applicant, Legal Services and the SRO as required to secure the appropriate approvals.

63. In urgent cases (i.e. a likelihood of endangering life or jeopardising an investigation if authorisation is not immediate), verbal authorisation may be sought and authorisation recorded in writing. An urgent verbal authorisation may last for 72 hours. However, if the surveillance continues and there is opportunity before the expiration of 72 hours, authorisation in writing should be applied for and authorised if appropriate.

64. Written authorisations for directed surveillance last for a fixed duration of three months and CHIS for 12 months (or one month in the case of a juvenile CHIS) from the date of the magistrate's approval. The Council will apply the same duration to non-RIPA authorisations.

65. Written authorisations for non-RIPA applications will be considered by the SIRO as authorising officer.

Conduct of authorisation

66. It will be the responsibility of the applicant and those conducting the authorised surveillance to ensure that it is done appropriately, ensuring:

    - surveillance is carried out in accordance with the authorisation;
    - collateral intrusion is monitored and minimised as far as possible;
    - intrusive surveillance is not carried out under any circumstances; and
    - information obtained is recorded and managed appropriately.

67. Any CHIS (RIPA only) used must be aware that:

    - only the tasks authorised must be carried out;
    - collateral intrusion is minimised as far as possible;
    - intrusive surveillance is not carried out under any circumstances
    - entrapment is not permitted; and
    - they must report only to the applicant.

68. If the authorised activity unexpectedly interferes with the privacy of individuals not covered by the authorisation, if the conduct or health safety of a CHIS becomes a concern, or any other unforeseen event occurs, the applicant must report this to the authorising officer, who will consider whether the authorisation should be amended or cancelled.

Review

69. All authorisations for covert surveillance or use of a CHIS (RIPA only) will be reviewed by the applicant using the appropriate form every 28 days, or sooner if

the risk of collateral intrusion or of obtaining private information is high or the circumstances of the investigation require it.

70. The applicant will send the completed form to the relevant authorising officer and the coordinating officer.

Renewal

71. If towards the end of the authorisation period there is a case for continuing the covert surveillance, the applicant will complete the appropriate form and send to the relevant authorising officer for consideration.

72. If the authorising officer agrees that the grounds for authorisation remain in place then the form will be sent to the coordinating officer to arrange consideration by a JP for RIPA applications.

73. If the authorisation lapses during this period then no further surveillance can be undertaken until the JP has approved the renewal for RIPA applications.

74. Subject to approval, directed surveillance can be extended for a further three months and an adult CHIS for a further 12 months, starting on the date of the day the previous authorisation ended.

75. For non-RIPA applications, renewal applications for surveillance will be considered by the SIRO as authorising officer.

Cancellation

76. There is a presumption that covert surveillance or CHIS authorisations (RIPA only) will be cancelled at the earliest opportunity using the appropriate form.

77. Authorisations ***must*** be cancelled if the authorisation period has not ended and:

    - conditions for authorising the surveillance are no longer satisfied;
    - sufficient information has been gathered to progress litigation; or
    - it is clear that no evidence of the suspected activity will be detected.

78. Authorisations must also be cancelled when the authorisation period has expired and a renewal has not been requested and authorised.

79. The applicant will send the completed form to the relevant authorising officer and the coordinating officer.

Errors

80. All errors in documentation must be reported immediately by the authorising officer to the SRO for consideration and appropriate action.

Covert Human Intelligence Sources (CHIS)

81. The Council will use CHIS to acquire information covertly where it is lawful and appropriate to do so. The crime threshold does not apply to the authorisation of a CHIS.

82. Individuals contacting the Council to provide unsolicited information on a one-off basis will not be considered CHIS.

83. Similarly, those individuals undertaking test purchases on behalf of the Council will be trained to ensure that they do not form a relationship other than that of customer / retailer, and these individuals will also not be considered CHIS.

84. If however that individual proceeds to pass on more information and this includes forming a relationship with other parties to facilitate this, then a CHIS application will be made. Officers must be conscious of the prospect of individuals drifting into the status of CHIS in their desire to assist the Council and take appropriate actions to advise and safeguard such individuals where necessary.

85. The Council will not authorise the use of a juvenile as a CHIS against their parents or carers. The Council will not authorise the use of a juvenile or a vulnerable adult as a CHIS without undertaking a specific risk assessment. Authorisation of such an individual as a CHIS can only be approved by the Head of Paid Service. Forms set out at appendices 7 to 10 of this policy set out the detail required for the approval, review and cancellation of CHIS surveillance requests.

Other third parties

86. Where the Council has instructed another agency to act on its behalf under RIPA, this policy and its associated procedures and forms will apply. Applicants will ensure that third parties are aware of exactly what they are authorised to do.

87. Two or more public authorities can undertake a joint directed surveillance investigation or use of a CHIS. In such circumstances it must be clear which authority will lead the investigation and so authorise the surveillance.

88. Requests from third parties to use the Council's equipment, facilities and / or buildings under RIPA authorisations must be made in writing (including a copy of the authorisation, redacted where appropriate) to the SRO, or in the case of CCTV, the SPoC.

Telecommunications data

89. The Council can apply for individual's telecommunications data in support of investigations where appropriate. Applications can be made for entity and event data. The crime threshold applies only to event data.

90. Applicants for telecommunications data must complete the appropriate forms, which will be provided by the Designated Person. Applications will be routed

through the IPA SPOC, NAFN, which will check for legal compliance and submit applications to the OCDA once approved by the Council's Designated Person.

91. Any application returned by the OCDA for re-work must be completed within 14 days or a new request must be submitted. Any application rejected by the OCDA can be appealed within seven days, via the Designated Person.

Online surveillance

92. Websites and social media are another source of intelligence for investigations.

93. In general terms, overt monitoring of online material, where the subject has been informed that this is taking place, or the preliminary reconnaissance by Council officers of websites or the social media sites of individuals to ascertain whether they may be of interest, and that do not involve any personal interaction, will be unlikely to require authorisation as they are unlikely to interfere with an individual's reasonably held expectation of privacy.

94. In all other circumstances (e.g. repeated visits to sites to gather information, or establishing a relationship with a viewing to purchasing items either directly or through a CHIS) will likely require authorisation as set out in this policy.

95. Officers will not use covert profiles online. If an investigation requires covert profiles then this should be undertaken by the police or specialists in regional or national trading standards teams.

96. The Council will set out in its privacy notices where it may gather information from online sources as part of its investigations, including the lawful condition relied upon.

97. In undertaking online surveillance, officers will have regard to the relevant code(s) of practice, the Council's covert surveillance procedure and associated guidance, and be advised by the SRO, Coordinating Officer (Auditor) and / or Legal Services where required.

Surveillance of employees

98. All employees are entitled to a comfortable working environment that provides an appropriate degree of privacy, consistent with data protection legislation. However, the monitoring of employees is necessary under certain circumstances in order to safeguard employees, customers and the Council as an employer.

99. The Council will be clear with employees and Trade Unions when, under what circumstances and to what extent, monitoring and surveillance – both overt and covert – will be used in the workplace.

100. All monitoring and surveillance of employees will be proportionate and in line with the guidance issued by the Information Commissioner to ensure employees' personal data is respected and properly protected under the data protection legislation. In order to lawfully monitor employees, the Council must identify its

lawful basis for doing so and identify a special category processing condition if sensitive data is likely to be captured. The Information Commissioner's Office provides an interactive tool to support applicants to understand the lawful basis for planned monitoring.[1]

101. Employees will be routinely captured on CCTV during the course of their work. Some employees have been given access to devices which offer the option of using biometric data to secure the device. Where an employee has opted into that device, any data gathered will be held on the device and only used for that purpose.

102. The Council will also collate and retain records of employee communications data, including but not limited to, door entry, vehicle, safety tracking devices, ICT device, network, system and internet access and usage, instant messaging, telephone calls and printing logs, in line with its retention schedule.

103. Employees will be clearly advised as to what represents appropriate and fair private usage of the systems set out above. In some cases the Council will not permit the private use of such systems at all.

104. The content of phone calls and online meetings involving employees will only be recorded where there is prior notification to the caller e.g. into the Council's contact centre.

105. The Council will use GPS trackers on all of its fleet vehicles and also provide them to certain individuals in line with their job roles or working arrangements e.g. neighbourhood wardens, lone workers. Alertcom users.

106. The Council will not track any individual through their work-provided mobile phone or other devices unless there is considered to be a threat to the individual's or other relevant person's health and safety or tracking is incidental e.g. attempting to locate a device that has been reported as lost, missing or stolen.

107. The Council will undertake drug and alcohol testing for employees where there is reasonable cause and post-incident (e.g. after a road traffic accident).

108. CCTV footage of employees may be used to investigate a crime or incident of anti-social behaviour, or to investigate a security or health and safety incident.

109. Employee communications will be legitimately accessed and utilised in the investigation of management investigations, complaints and in response to statutory information requests from members of the public.

110. Routine monitoring of systems access will be undertaken to ensure that employee access to customer personal data is lawful and appropriate.

[1] https://ico.org.uk/for-organisations/gdpr-resources/lawful-basis-interactive-guidance-tool/

111. Outside of the above, access to internal CCTV footage and employee communications data and the covert surveillance of employees through these means will only be permitted where it complies with Human Rights and associated legislation, specifically during an investigation of an allegation of a serious disciplinary offence and will be authorised by the HR Manager as part of the Council's disciplinary procedure.

112. Employee information will only be accessed by those with a business need to know. Any personal information collected in the course of monitoring or surveillance that is not in line with the purposes described above will not be accessed, unless it is required or permitted by law. A form is in place that sets out the detail required for the authorisation, review and cancellation of employee covert surveillance which should only be used in exceptional circumstances and in line with guidance from the ICO.

Non-RIPA surveillance of the public and third parties

113. Paragraph 68 of this policy sets out that in exceptional circumstances the Council will carry out covert surveillance to progress investigations outside of the RIPA framework, where (i) while significant, the matters under investigation may not typically result in criminal proceedings, or (ii) the potential criminal offence(s) under investigation are likely to attract a penalty below the RIPA threshold. The form for this process must be completed and submitted to the SRO for approval before non-RIPA covert surveillance of third parties or the public is conducted.

114. Surveillance under this policy section must be conducted with a view to minimising data collected and minimising the length of time surveillance is conducted for. A maximum of 30 days can be approved at any one time.

Equipment

115. All equipment used by the Council will be fit-for-purpose, inspected and maintained to schedule and produce video and audio footage and images to the appropriate evidential standard.

116. Where CCTV cameras are used covertly as part of an operation to observe a targeted individual or group, the appropriate authorisation must be applied for.

117. Equipment for the purposes of covert surveillance will only be installed when the required authorisations and approvals have been obtained by the case worker, as set out in this policy.

118. Covert surveillance equipment will only be installed in residential premises if prior written permission has been obtained from the householder.

119. Equipment and surveillance logs will be allocated from a central record of equipment, and an appropriate audit trail maintained. Upon cancellation all equipment in use must be removed immediately or else as soon as practicable, since further recordings will amount to unauthorised surveillance.

Evidence handling and records management

120. Evidence gathered during the course of overt and covert surveillance will include electronic and paper files and records, video and audio recordings, photographs and negatives.

121. Material gathered as part of surveillance activities will not be used for any purpose other than that authorised. Where surveillance gathers information that may be relevant to other criminality, the Council may disclose this to appropriate law enforcement agencies, in line with data protection legislation.

122. The Council's privacy notices will set out what personal information services may gather from surveillance activities.

123. Evidence gathered during surveillance will be handled, stored and disseminated safely and securely in line supporting procedures and the Council's retention schedule:

- CCTV images will be retained for 28 days;
- covert surveillance records will be retained for seven years;
- additional records will be retained for CHIS; and
- any material that may be relevant to pending or future litigation will be retained until such litigation is concluded, and thereafter subject to periodic review.

124. Where material is obtained unrelated to the investigation and there is no reason to suspect that it will be relevant to any future litigation, it will be destroyed at the earliest opportunity.

125. The Coordinating Officer (Auditor) will maintain a detailed central record of applications, authorisations, orders, reviews, renewals and cancellations, together with supporting documentation. This will be held in the Council's EDRMS in order to facilitate effective records management across the lifecycle.

Roles and Responsibilities

126. Effective and lawful surveillance is the collective responsibility of all those individuals named within the scope of this policy. Appropriate training will be provided to all those officers within the scope of this policy.

127. As with all Council policies, Directors and Heads of Service have a general responsibility to ensure compliance with this policy within their operations. This includes taking reasonable steps to protect the health and safety and where appropriate third parties involved in surveillance, including the carrying out of risk assessments.

128. The specific roles within surveillance activities are described below. Where appropriate, the current role holders and their deputies are listed at Appendix 2.

Senior Responsible Officer (SRO)

129. The SRO has overall responsibility for overt and covert surveillance, including:

- creation, communication and review of this policy;
- appointing the CCTV Single Point of Contact;
- appointing the Coordinating Officer (Auditor) for covert surveillance;
- ensuring the availability of appropriate authorisers for covert surveillance;
- raising corporate awareness of the policy and proper surveillance practices;
- assessing corporate compliance with this policy;
- providing professional guidance on all matters relating to surveillance;
- engagement with the Surveillance Camera Commissioner and the IPCO; and
- overseeing the implementation of any post-inspection action plans recommended or approved by the IPCO.

Overt surveillance

130. The following key roles are in place in relation to **overt** surveillance via cameras and other equipment:

CCTV Single Point of Contact (SPOC)

131. Appointed by the SRO, and supporting the Data Protection Officer, the SPOC will ensure the Council operates all surveillance camera equipment in compliance with the Surveillance Camera Code and key legislation, thereby building transparency, trust and confidence.

132. Specifically, the SPOC will:

- establish and maintain a CCTV code of practice setting out the regulatory framework that each Council scheme must comply with, the internal assessment programme that each scheme must undertake and the processes required to establish a new surveillance camera scheme or upgrade an existing scheme;
- maintain a central register of all public space surveillance camera equipment operated by the Council, including the location of each piece of equipment, its asset reference and the manager responsible;
- act as the main point of contact for surveillance camera systems, and introduce consistent procedures that can be applied across all systems in operation, including standardised signage, alongside appropriate training for those operating surveillance cameras; and
- provide regular guidance and updates to scheme managers to ensure that all surveillance cameras schemes continue to operate in full compliance with the regulatory framework governing its use and undertake an annual audit of all schemes, documented in an annual report to the SRO.

Scheme Managers

133. A scheme manager will be in place for each individual scheme operated by or on behalf of the Council. Scheme managers will maintain the following documentation in a Code Assessment Pack, which will demonstrate compliance with the local code and allow the SPOC to undertake their role.

- list of all documents maintained by the scheme manager;
- scheme asset list – a complete record of all cameras, signage, monitors and recording equipment, with location, functionality and purpose and associated contractual arrangements for management and / or maintenance;
- record of data protection impact assessments (DPIAs) for each camera (or if agreed, groups of cameras) on the asset list and cyber security checks undertaken;
- scheme access list – including who is authorised to access the scheme and the level of access granted;
- training records of all those accessing the scheme and associated confidentiality arrangements;
- records of the self-assessment and annual review, including who undertook this and the changes made as a result; and
- declaration of compliance – completed annually or when the scheme manager changes.

Responsible Officers

134. All CCTV sites also should have an appointed Responsible Officer (RO) – this may or may not be the scheme manager. ROs are responsible for the day-to-day management of the CCTV system and providing relevant information to the scheme manager.

Surveillance Camera Operators

135. All surveillance camera operators or those otherwise viewing images will undertake training relevant to operating public space surveillance, information security and personal data. They will be required to sign appropriate confidentiality agreements.

Covert surveillance

136. The following key roles are in place in relation to **covert** surveillance:

Coordinating Officer (Auditor)

137. The Coordinating Officer (Auditor) will:

- provide up-to-date guidance and training on covert surveillance within the Council;
- maintain a central record of authorisations including a Unique Reference Number (URN);

- audit each covert surveillance application, authorisation, review, renewal and cancellation for compliance with this policy and the law, ensuring there is a uniformity of practice; and
- advise the SRO as appropriate in the light of the above.

Authorising Officers

138. Authorising Officers will assess, authorise, renew and cancel all public-facing covert surveillance (RIPA or non-RIPA) on behalf of all Directorates. Authorising Officers will be at Head of Service level or above, trained to an appropriate standard, and cannot authorise surveillance requested by any service or team under their management.

139. The SRO will ensure there is always a minimum of three trained authorising officers within the Council. The SRO will authorise surveillance in exceptional circumstances.

140. If confidential information or matters subject to legal privilege are likely to be acquired through directed surveillance or by a Covert Human Intelligence Source (CHIS), or the CHIS is a juvenile aged between 16-18 years or a vulnerable adult, the surveillance may only be authorised by the Head of Paid Service.

141. Covert surveillance of employees will only be permitted during an investigation of an allegation of a serious disciplinary offence and will be authorised by the HR Manager and an authorising officer. A form is in place to ensure compliance with this policy for non-RIPA directed surveillance.

IPA Single Point of Contact (SPoC) (Communications data)

142. The National Anti-Fraud Network (NAFN) acts as the SPoC for the Council for the acquisition of external communications data, liaising with the Office for Communications Data Authorisations on the Council's behalf.

IPA Designated Person (Communications data)

143. The Designated Person (Communications data) approves telecommunications applications that have been checked by the IPA SPoC.

Applicants (Case Officers)

144. Only officers that can reasonably be expected to undertake covert surveillance as part of their job description will plan and apply for the authorisation of such surveillance for RIPA based surveillance. Line Managers may apply to conduct non-RIPA based surveillance of an employee by accessing communications, tracking or other data but must have the approval of the HR Manager, unless there is a reason why they should not be made aware of the surveillance. In that case the reason must be set out in the application and the approval of the SRO sought. In some restricted circumstances, there may be a need to consider covert surveillance of the public in circumstances where the RIPA

threshold would not be met but the Council may have a legitimate need to gather information in order to assess fraud, defend a legal case or investigate in line with its statutory duties. Where this is the case, an authorisation process must be followed where the need to gather evidence would exceed the threshold for surveillance.

Supporting policies, procedures, and standards

145. The following supporting procedures and guidance will be made available in support of this policy:

- CCTV Code of Practice
- CCTV Code Assessment Pack
- Covert surveillance procedure
- Fleet vehicle tracking procedure
- Drug and alcohol testing procedure.

146 Each procedure will be subject to impact assessment, including data protection impact assessment, and privacy notices will be updated accordingly.

Monitoring and review arrangements

147 This policy will be reviewed on an annual basis, considered by the appropriate Scrutiny Panel(s) and approved by the Executive. The policy and, where appropriate supporting procedures, will be made available on the Council's Open Data site.

148 Ongoing monitoring will be undertaken by the SPoC (overt surveillance) and the Coordinating Officer (Auditor) (covert surveillance) to ensure organisational compliance with this policy on a live basis. Any issue arising will be reported to the SRO and the Council's Risk Management Group and Corporate Governance Board will be updated as appropriate.

149 The Corporate Affairs and Audit Committee is responsible for oversight of the Council's corporate governance processes. To ensure appropriate oversight of surveillance is maintained, an overview of applications, compliance and trends will be provided to the Committee within an annual report from the SRO.

150 Data relating to the Council's overt and covert surveillance activity (redacted as appropriate) will be published annually on the Council's Open Data site.

151 Statistical returns for CCTV will be submitted to the Surveillance Camera Commissioner by the SRO upon request. The SRO will comply with requests from the Surveillance Camera Commissioner in relation to the organisation of inspections of the Council.

152 Statistical returns for directed surveillance and communications acquired using RIPA will be submitted to the IPCO by the SRO upon request. The SRO will

comply with requests from the IPCO in relation to the organisation of inspections of the Council.

Complaints

153 Complaints relating to any surveillance matters must be made in writing and addressed to:

Senior Responsible Officer (Surveillance)
Middlesbrough Council
PO Box 500
Middlesbrough
TS1 9FT

154 Complaints will be investigated in line with the Council's complaints policy and where appropriate the Council's data protection policies. All alleged breaches of privacy will be investigated and appropriate action taken.

155 If the complainant remains dissatisfied following the SRO's response they will if appropriate be advised to write to the Local Government and Adult Social Care Ombudsman and / or the Information Commissioner's Office as appropriate.

156 If the complaint relates to covert surveillance, complainants will also have recourse to:

The Investigatory Powers Tribunal
PO Box 33220
London SW1H 9ZQ
Tel. 0207 035 3711

157 Costs incurred by the Council as a result of cases progressed to The Investigatory Powers Tribunal or the courts, will be met by the relevant Directorate.

Appendix 1: Definitions

Surveillance

Monitoring, observing or listening to persons, their movements, conversations or other activities and communications. Surveillance may be conducted with or without the assistance of a surveillance device and includes the recording of any information monitored, observed or listened to during the course of surveillance.

Overt surveillance

Surveillance that is intentionally and visibly undertaken. General observations made by officers in the course of their duties constitutes overt surveillance. Surveillance by visible cameras e.g. CCTV, body worn cameras and automatic number plate recognition cameras is also overt surveillance and must be appropriately signed.

Covert surveillance

Surveillance is covert if, and only if, it is carried out in a manner calculated to ensure that any persons who are subject to the surveillance are unaware that it is or may be taking place. There are three types of covert surveillance: directed surveillance, covert human intelligence sources, and intrusive surveillance.

Directed surveillance

Surveillance is directed if it is covert, but not intrusive, and is undertaken for the purposes of a specific investigation or operation and in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation).

Surveillance will not be directed, and therefore will not require authorisation, if it is done by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation to be sought for carrying out the surveillance.

Covert Human Intelligence Source (CHIS)

A person who establishes or maintains a personal or other relationship with a person and:

- covertly uses such a relationship to obtain information or provide access to any information to another person, or
- covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

Intrusive surveillance

Surveillance is intrusive if it is covert surveillance that (a) is carried out in relation to anything taking place on any residential premises or in any private vehicle; and (b)

involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

Local authorities are not permitted to carry out intrusive surveillance in any circumstances.

Private information

Information capable of including any aspect of a person's private or personal relationship with others, such as family and professional or business relationship. Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public.

Collateral intrusion

The risk of intrusion into the privacy of persons other than the target of covert surveillance.

Confidential information

Consists of matters subject to legal privilege, confidential journalistic material, constituent information and confidential personal information which is held in confidence about the physical or mental health or spiritual counselling of a person (whether living or dead) who can be identified from it.

Residential premises

Any premises as is for the time being occupied or used by any person, however temporarily, for residential purposes or otherwise as living accommodation. This includes hotel rooms or rented flats but not communal areas, front gardens, hotel reception areas or dining rooms or driveways readily visible to the public.

Private vehicles

Any vehicle which is used primarily for the private purposes of the person who owns it or a person otherwise having the right to use it. This includes leased and company cars.

Communications data

Information about communications: the 'who', 'where' 'when', 'how', and 'with whom' of a communication but not what was written or said (i.e. not content). Generally, it is data that may be acquired from a Telecommunication Operator (TO) as per below.

Entity data (as per the Communications Data Code of Practice 2018)

Data regarding the use of service(s) by customers, including:

- subscriber checks' such as "who is the subscriber of phone number 01234 567 890?", "who is the account holder of e-mail account example@example.co.uk?" or "who is entitled to post to web space www.example.co.uk?";
- subscribers' or account holders' account information, including names and addresses for installation, and billing including payment method(s), details of payments;
- information about the connection, disconnection and reconnection of services to which the subscriber or account holder is allocated or has subscribed (or may have subscribed) including conference calling, call messaging, call waiting and call barring telecommunications services;
- information about apparatus or devices used by, or made available to, the subscriber or account holder, including the manufacturer, model, serial numbers and apparatus codes; and
- information about selection of preferential numbers or discount calls.

Event data

Identifies or describes events in relation to a telecommunication system which consist of one or more entities engaging in an activity at a specific point, or points, in time, including:

- information tracing the origin or destination of a communication that is, or has been, in transmission (including incoming call records);
- information identifying the location of apparatus when a communication is, has been or may be made or received (such as the location of a mobile phone);
- information identifying the sender or recipient (including copy recipients) of a communication from data comprised in or attached to the communication;
- routing information identifying apparatus through which a communication is or has been transmitted (for example, file transfer logs and e-mail headers – to the extent that content of a communication, such as the subject line of an e-mail, is not disclosed);
- itemised telephone call records (numbers called);
- itemised internet connection records;
- itemised timing and duration of service usage (calls and/or connections);
- information about amounts of data downloaded and/or uploaded;
- information about the use made of services which the user is allocated or has subscribed to (or may have subscribed to) including conference calling, call messaging, call waiting and call barring telecommunications services.

Local authorities are prohibited from acquiring internet connection records for any purpose.

National Anti-Fraud Network (NAFN)

A not-for-profit public sector organisation providing a range of data and intelligence services that are subscribed to by over 90% of local authorities. NAFN acts as the Council's Single Point of Contact for the acquisition of external communications data, liaising with the Office for Communications Data Authorisations on the Council's behalf.

Office for Communications Data Authorisations (OCDA)

Created under the IPA, the Office for Communications Data Authorisations considers requests for communications data from law enforcement and public authorities.

Surveillance Camera Commissioner

The role of Surveillance Camera Commissioner (Professor Fraser Sampson) was created under POFA to encourage compliance with the surveillance camera code of practice, review how the code is working, and provide advice to ministers on whether or not the code needs amending.

Investigatory Powers Commissioner's Office (IPCO)

Overseen by the Investigatory Powers Commissioner (Sir Brian Leveson), the IPCO was created under the IPA to provide independent oversight and authorisation of the use of investigatory powers by intelligence agencies, police forces and other public authorities.

Appendix 2: Key officers

Senior Responsible Officer (SRO)

Ann-Marie Johnstone, Head of Governance, Policy and Information
Deputy: Leanne Hamer, Governance and Information Manager

CCTV Single Point of Contact (SPoC)

John Kirk, Service Delivery Manager

Coordinating Officer (Auditor)

Leanne Hamer, Governance and Information Manager
Deputy: Michael Brearley, Data Protection Officer (for compliance audit purposes only)

Authorising Officers

Richard Horniman, Director of Regeneration and Culture
Judith Hedgley, Head of Public Protection
Claire Holt, Head of Strategic Housing

Authorising officers deputise for one another.

Authorising Officer for Juvenile / Vulnerable Adult CHIS, or where confidential information or matters subject to legal privilege are likely to be acquired through either directed surveillance or by a CHIS

Louise Grabham, Director of Adult Social Care and Public Health

Designated person

Judith Hedgley, Head of Public Protection
Deputy: Ann-Marie Johnstone, Head of Policy, Governance and Information

Non-RIPA Staff surveillance authorising officer

HR Manager, Kerry Rowe.

Impact Assessment Level 1: Initial screening assessment **Appendix 3**

Subject of assessment:	Surveillance Policy 2025-26			
Coverage:	Overarching / crosscutting			
This is a decision relating to:	☐ **Strategy**	☒ **Policy**	☐ **Service**	☐ **Function**
	☐ **Process/procedure**	☐ **Programme**	☐ **Project**	☐ **Review**
	☐ **Organisational change**	☐ **Other (please state)**		
It is a:	**New approach:**	☐	**Revision of an existing approach:**	☒
It is driven by:	**Legislation:**	☒	**Local or corporate requirements:**	☒
Description:	**Key aims, objectives and activities** The proposed policy provides a framework for the undertaking surveillance activities across the Council in compliance with all applicable laws by. **Statutory drivers** Human Rights Act 1998, Regulation of Investigatory Powers Act 2000, UK General Data Protection Regulation, Data Protection Act 2018, Protection of Freedoms Act 2012, Investigatory Powers Act 2016 **Differences from any previous approach** This policy supersedes the previous policy for 2024/25, setting out the Council's policy in relation to CCTV, non-RIPA surveillance and employee surveillance, amongst other matters. **Key stakeholders and intended beneficiaries (internal and external as appropriate)** Elected members, employees of the Council, local communities and businesses, partners, regulators. **Intended outcomes** To ensure that the Council's approach to surveillance clearly articulated and communicated to all stakeholders, and that the Council continues to comply with its legal duties.			
Live date:	December 2025			
Lifespan:	December 2025 – December 2026			
Date of next review:	Reviewed on an annual basis – December 2026			

Screening questions	Response			Evidence
	No	Yes	Uncertain	
Human Rights Could the decision impact negatively on individual Human Rights as enshrined in UK legislation?*	☒	☐	☐	No. The policy is specifically designed to ensure that human rights as identified in national legislation is not contravened when undertaking surveillance activities. Evidence used to inform this assessment includes analysis of legislation, statutory and draft statutory guidance and feedback from the IPCO inspection regime.
Equality Could the decision result in adverse differential impacts on groups or individuals with characteristics protected in UK equality law? Could the decision impact differently on other commonly disadvantaged groups?*	☒	☐	☐	No. The policy will ensure a systematic and evidence-based approach to surveillance undertaken in communities and in the workplace. As a result there are no concerns that the actions could have a disproportionate adverse impact on groups or individuals with characteristics protected in national legislation. Evidence used to inform this assessment includes analysis of legislation, statutory and draft statutory guidance and feedback from the IPCO inspection regime.
Community cohesion Could the decision impact negatively on relationships between different groups, communities of interest or neighbourhoods within the town?*	☒	☐	☐	No. The policy will ensure a systematic and evidence-based approach to surveillance undertaken in communities and in the workplace. Specific account will be taken in appropriate assessments of community sensitivities. As a result there are no concerns that the proposed plan could have an adverse impact on community cohesion. Evidence used to inform this assessment includes analysis of legislation, statutory and draft statutory guidance and feedback from the IPCO inspection regime.

Screening questions	Response			Evidence
	No	Yes	Uncertain	
Armed Forces Could the decision impact negatively on those who are currently members of the armed forces of former members in the areas of Council delivered healthcare, compulsory education and housing policies?*	☒	☐	☐	No. The policy will ensure a systematic and evidence-based approach to surveillance undertaken in communities and in the workplace. Specific account will be taken in appropriate assessments of community sensitivities. As a result there are no concerns that the proposed plan could have an adverse impact on community cohesion. Evidence used to inform this assessment includes analysis of legislation, statutory and draft statutory guidance and feedback from the IPCO inspection regime.
Care leavers Could the decision impact negatively on those who are care experienced?*	☒	☐	☐	No. The policy will ensure a systematic and evidence-based approach to surveillance undertaken in communities and in the workplace. Specific account will be taken in appropriate assessments of community sensitivities. As a result there are no concerns that the proposed plan could have an adverse impact on this group. Evidence used to inform this assessment includes analysis of legislation, statutory and draft statutory guidance and feedback from the IPCO inspection regime.
Reducing Poverty Could the decision impact negatively on the Council's ambitions to reduce poverty in the town?	☒	☐	☐	No. The policy will ensure a systematic and evidence-based approach to surveillance undertaken in communities and in the workplace. Specific account will be taken in appropriate assessments of community sensitivities. As a result there are no concerns that the proposed plan could have an adverse impact on this group. Evidence used to inform this assessment includes analysis of legislation, statutory and draft statutory guidance and feedback from the IPCO inspection regime.

Assessment completed by:	Leanne Hamer Governance & Information Manager	**Head of Service:**	Ann-Marie Johnstone, Head of Policy, Governance and Information
Date:	17/11/2025	**Date:**	27/11/2025

This page is intentionally left blank

MIDDLESBROUGH COUNCIL	Middlesbrough moving forward

Report of:	Charlotte Benjamin - Director of Legal and Governance Services
Relevant Executive Member:	Chris Cooke - Mayor
Submitted to:	Single Member Executive – The Mayor
Date:	18 December 2025
Title:	Artificial Intelligence (AI) Policy 2025 – 2028
Report for:	Decision
Status:	Public
Council Plan priority:	Delivering Best Value
Key decision:	No
Why:	Decision does not reach the threshold to be a key decision
Subject to call in?	Yes
Why:	Non-Urgent Report

Proposed decision(s)

That the Mayor:

- **APPROVES** the adoption of the Artificial Intelligence (AI) Policy 2025 – 28
- **APPROVES** that the Head of ICT and Digital has authority to make changes to the policy, following consultation with the Council's Senior Information Risk Owner (SIRO), to ensure the policy keeps pace with emerging AI technology, legislation, case law and guidance from government.

Executive summary

This report introduces Middlesbrough Council's Artificial Intelligence (AI) Policy, developed to ensure the lawful, ethical, and responsible use of AI technologies across the organisation.

The policy recognises the growing role of AI in supporting public service delivery and outlines a clear framework to guide its use in a way that enhances productivity while safeguarding data, upholding transparency, and maintaining human accountability. The policy sets out that AI must never replace human judgement. All decisions remain the responsibility of Council officers or elected Members, and AI may only be used to support, not replace, human decision-making. The policy also mandates training for all

staff using AI tools and sets clear expectations for suppliers providing AI-enabled systems.

The vision underpinning the policy is that AI will be used to support the Council's strategic priorities in a way that is ethical, secure, and transparent, giving assurance to residents, staff, and partners.

The policy is structured around the following key principles:

- Human accountability and oversight
- Safe and ethical use of AI tools
- Secure access and device control
- Clear boundaries for permitted and prohibited use
- Supplier compliance and transparency

This policy forms part of the Council's wider Information Governance and Digital Strategy framework. It will be reviewed at least annually by the Head of ICT and Digital, in conjunction with the Information Governance and Technology Design Authority Board, to ensure it remains current and responsive to emerging technologies and risks.

1. Purpose of this report and its contribution to the achievement of the Council Plan ambitions.

1.1 The purpose of this report is to set out a proposed Artificial Intelligence (AI) Policy for Middlesbrough Council. As AI technologies become increasingly embedded in public service delivery, it is essential that the Council adopts a clear and robust framework to guide their use.

1.2 This report outlines the rationale for adopting an AI Policy that ensures AI is used lawfully, ethically, and responsibly, in a way that supports the Council's strategic priorities and maintains public trust. The policy sets out the principles, expectations, and governance arrangements for the use of AI across the organisation.

1.3 The AI Policy contributes to the Council Plan ambitions by enabling the safe and effective use of AI to improve productivity, enhance service delivery, and support innovation, while ensuring that human accountability, data protection, and ethical standards remain central to all AI-related activity.

1.4 A Member decision is required, as the adoption of an Artificial Intelligence (AI) Policy falls within the Executive Member for LGS, Mayor Chris Cooke remit to approve policies that govern the Council's use and management of digital technology.

Our ambitions	Summary of how this report will support delivery of these ambitions and the underpinning aims
A successful and ambitious town	The AI Policy will support the Council to achieve it ambitions in these areas by promoting ethical and secure use of data and technology to improve services and protect residents. By embedding human decision making and clear
A healthy Place	
Safe and resilient communities	

	governance, it supports innovation while ensuring compliance.
Delivering best value	The AI Policy will support digital transformation by enabling the Council to adopt AI tools that improve service efficiency, responsiveness, and innovation, ensuring services are better tailored to the needs of residents and businesses.

2. Recommendations

2.1 That the Mayor:

- **APPROVES** the adoption of the Artificial Intelligence (AI) Policy 2025 – 28
- **APPROVES** that the Head of ICT and Digital has authority to make changes to the policy, following consultation with the Council's Senior Information Risk Owner (SIRO), to ensure the policy keeps pace with emerging AI technology, legislation, case law and guidance from government.

3. Rationale for the recommended decision(s)

3.1 Having a clear policy in place to guide the use of AI is essential for a modern, complex organisation. AI technologies present significant opportunities to improve productivity, streamline operations, and enhance service delivery. However, without appropriate governance, they also introduce risks related to data protection, ethics, and accountability. A decision from the Mayor is sought as the agenda item is within their portfolio.

3.2 This policy ensures that AI is used in a way that aligns with the Council's strategic priorities, supports innovation, and maintains compliance with legal and ethical standards. By embedding human decision making and clear governance, the policy provides a basis that enables the Council to adopt AI confidently and responsibly.

4. Background and relevant information

4.1 The AI Policy is aligned with the Council's existing Information Governance framework and wider digital ambitions.

4.2 The policy provides a framework to ensure that AI technologies are used lawfully, ethically, and effectively to support service delivery, innovation, and operational efficiency, while maintaining human oversight and accountability.

4.3 The AI Policy supports the Council's digital ambitions by enabling the safe and appropriate use of AI tools to enhance how services are delivered. It ensures that emerging technologies are adopted in a way that is secure and aligned with the Council's values and priorities.

4.4 An effective AI Policy will deliver the following benefits:

- Enable safe and responsible use of AI
- Ensure compliance with data protection, equality, and ethical standards
- Maintain human accountability in all decision-making processes

4.5 The AI Policy sets out:

- Responsible and appropriate use of AI across Council services
- How AI will be used appropriately within the Council
- Guidance on appropriate and ethical use of AI in Council operations
- Ensuring AI is used appropriately

4.6 The policy also outlines the Council's approach to due diligence when considering new AI tools. Where AI functionality is proposed, either as standalone solutions or embedded within third-party systems, ICT will work closely with the relevant service leads to assess the value, risks, and implications before implementation. This includes evaluating the purpose, data requirements, ethical considerations, and governance needs of the proposed AI functionality.

4.7 Following adoption, the policy will be overseen by the Head of ICT and Digital. The policy will be reviewed at least annually to reflect emerging technologies, risks, and best practice, with major changes referred to Members for approval.

5. Ward Member Engagement if relevant and appropriate

5.1 Not applicable to this report.

6. Other potential alternative(s) and why these have not been recommended

6.1 The Council could choose to operate without a formal AI Policy. However, in the context of increasing use of AI technologies across the public sector, the absence of a clear policy would present significant risks. These include inconsistent use of AI tools, potential non-compliance with data protection and ethical standards, and a lack of transparency or accountability in decision-making.

6.2 Setting out a clear and consistent approach to the use of AI provides a shared understanding across the organisation and with partners. It ensures that AI is used in a way that supports the Council's digital ambitions and helps deliver high-quality, ethical, and efficient services to residents and businesses in Middlesbrough.

7. Impact(s) of the recommended decision(s)

Topic	Impact
Financial (including procurement and Social Value)	The implementation of the AI Policy may have financial implications over time, particularly as new AI tools are assessed, procured, or integrated into existing systems. Any associated costs will be considered on a case-by-case basis and only progressed if the costs can be met through pre-existing budgets or the appropriate approval has been obtained, after which they will be further progressed through the Council's standard decision-making and procurement processes to ensure value for money and alignment with social value principles.

Legal Data Protection	This policy will ensure compliance with all applicable UK legislation and statutory guidance in relation to use of AI including: UK General Data Protection Regulation 2016 Data Protection Act 2018 Data (Use and Access) Act 2025 Equality Act 2010 Human Rights Act 1998 Freedom of Information Act (FOIA) 2000 Environmental Information Regulations 2004 Contract, Copyright, and Intellectual Property Law Statutory and recommended guidance
Risk	Implementation of the policy will contribute positively to the management of Strategic Risk Register item SRR 13: - (SRR 13) If the Council's Corporate Governance arrangements are not fit for purpose and appropriate action is not taken to rectify this at pace, this could result, censure from the Council's auditors within a public interest report that would damage the Council's reputation and/or in government formal intervention including removal of powers from officers and members and direction of council spend. The policy strengthens governance and accountability around the use of AI, reducing the risk of reputational damage or regulatory intervention.
Human Rights, Public Sector Equality Duty and Community Cohesion	The policy supports the Council's ability to demonstrate compliance with its duties in these areas by requiring ethical use of AI, transparency in decision-making. The policy will positively impact on human rights and will ensure compliance with the requirements of the Public Sector Equality Duty by requiring the completion of Equality Impact Assessments (EIAs) before an AI product is used that will process personal data. This will ensure that the Council does not introduce systems or processes that could impact unfairly on people or groups because they hold one or more protected characteristics.
Reducing Poverty Climate Change / Environmental Children and Young People Cared for by the Authority and Care Leavers	The policy enables better use of data and AI tools to support targeted service delivery and informed decision-making.

8. Actions to be taken to implement the recommended decision(s)

Action	Responsible Officer	Deadline
Publication of the Strategy	Head of ICT and Digital	30 January 2026
Establish internal guidance and resources for staff on AI use	Head of ICT and Digital and Head of Information Governance	30 January 2026
Develop and roll out AI awareness and training sessions	Head of ICT and Digital	30 January 2026

9. Appendices

1	Artificial Intelligence Policy 2025 - 2028

10. Background papers

Not applicable.

Contact: Lynsey Zipfell, Head of ICT and Digital

Email: Lynsey_Zipfell@middlesbrough.gov.uk

Artificial Intelligence Policy 2025 - 2028

Creator	Author(s)	Head of ICT and Digital		
	Approved by	Mayor Chris Cooke		
	Department	Legal and Governance Services		
	Service area	ICT and Digital Services		
Date	Created	November 2025		
	Submitted	December 2025		
	Approved	TBD		
	Updating Frequency	Annually, or sooner if changes to AI technologies, risks, or regulations arise		
Status	Final			
Contributor(s)	Head of ICT and Digital Head of Policy, Governance and Information Data Protection Officer Enterprise Architect Project Manager			
	Legislation	UK General Data Protection Regulation 2016 Data Protection Act 2018 Equality Act 2010		
Subject	ICT Applications			
Type	Policy			
	Vital Record	Yes	EIR	No
Coverage	Cross-cutting			
Language	English			

Document Control

Version	Date	Revision History	Reviser
1.0	First policy		

Distribution List

Version	Date	Name/Service Area	Action
1.0	All staff		

Contact:	Head of ICT and Digital

1. Purpose

This Artificial Intelligence (AI) Policy provides a framework for the lawful, ethical, responsible, and effective use of AI technologies by Middlesbrough Council. It is a living document and as such the Head of ICT and Digital, following consultation with the Senior Information Risk Owner, will make minor amendments to the policy during the life of the policy to reflect emerging changes to technologies, risks, or regulations as they arise. Major required changes will be returned to Members for decision.

Key expectations are that:

- AI must never replace human accountability. All final decisions remain the responsibility of Council officers or elected Members. AI may provide analysis, summaries, however human review, judgement and decisions is required in every case.
- All staff who use AI tools will be required to undertake training on safe and responsible AI use, including data protection, prompt management, and how to review and challenge AI outputs.
- Software suppliers providing AI solutions must comply with this policy, assist the Council in completion of its Data Protection Impact Assessment (DPIA) and Equality Impact Assessment (EIA), and provide assurances on ethical use, transparency, and data security.

This policy is designed to enable the effective and lawful use of AI to improve productivity while remaining fully compliant with ethical principles. It provides assurance to residents, staff, and businesses that their data will be handled ethically, safely, and transparently. The policy forms an element of the Council's Information Governance Policy Framework and supports delivery of the Digital Strategy vision.

2. Scope

This policy applies to:

- All staff, elected members, agency, volunteers working and commissioned services within Middlesbrough Council.
- All departments and services across the Council
- All AI systems used, develop, procured, pilot or deployed, including:
    - systems built or configured by the council.
    - systems purchase or licences from suppliers
    - systems being trailed or evaluated
    - AI features embedded within existing software platforms.

Device and Access Control

- All Council information systems, including AI tools, productivity platforms, applications, and data services must only be accessed on Council-issued and managed devices that meet corporate ICT security standards.
- The use of personal devices for Council systems is not permitted, unless formally authorised in writing by ICT Security and Information Governance.
- This requirement protects the security of Council data, ensures compliance with information governance obligations, and maintains accountability.
- All AI solutions and digital services, including associated data, must be accessed only through Council-approved environments and devices. Personal or unmanaged devices must not be used.

Permitted Use

AI may be used within Middlesbrough Council only when it supports lawful and ethical activity. Permitted uses include:

- Summarising information, generating draft reports or text, and assisting with communications.
- Supporting capturing content, processing requests, generating or logging routing queries.
- Productivity tasks such as document formatting, coding support, workflow automation or data classification.
- Analysing or processing datasets, documents or publicly available information to generate summaries, insights or comparisons in line with data protection legislation and Council policies.
- Use of AI tools that have been formally approved by the Council through Information Governance and the Technology Design Authority.
- All AI-generated outputs are to be review, validation, and approval by a human officer before use.

Prohibited Use

AI must not be used where it creates increases risk to individuals, data, or the Council. Prohibited uses include:

- Processing or sharing personal, confidential, or sensitive data in any public or unapproved AI tool.
- Treating AI outputs as authoritative or factual without verification by a trained officer.
- Using AI for automated decision-making about individuals that produces legal, financial, or significant personal effects, unless:
    - authorised by Information Governance and the Technology Design Authority,
    - supported by a DPIA, and EIA and
    - includes meaningful human review and the right to challenge.
- Deploying AI in a way that removes or replaces final human judgement.

Human oversight

All AI systems must include meaningful human oversight:

- A trained officer must review, challenge, and approve outputs before they are acted upon.
- Responsibility for decisions always remains with the human, not the AI system.

Third-Party Suppliers

All third-party suppliers and partners providing AI solutions, systems, or services on behalf of Middlesbrough Council must comply with this policy and with relevant legislation. Requirements for Suppliers:

- Suppliers must provide evidence that their AI systems comply with authority policies.
- Suppliers must disclose how their AI systems work, including training data sources, safeguards against bias, accuracy limits, and processes for human oversight.
- Suppliers must support the Council in completing or updating a DPIA and EIA and, before any AI functionality is enabled or procured.
- All contracts must include clear requirements for lawful use, transparency, supplier accountability, and Authority rights to audit and monitor compliance.
- If a supplier introduces or activates AI functionality in an existing or new system, the functional system owner must consult Information Governance to review and update the DPIA and EIA before the feature is enabled or the system is purchased.

3. Definitions

Topic	Definition
Artificial Intelligence (AI)	AI is a way of using computers to attempt to replicate human intelligence
Agentive AI	Refers to artificial intelligence systems designed to perform tasks autonomously on behalf of users. These systems can make decisions, take actions, and complete tasks without needing constant human intervention. They are often used to automate repetitive tasks, manage complex processes, or provide personalised assistance.
Generative Artificial Intelligence	Generative AI (GenAI) mimics intelligence by generating new outputs based on its training data, often seen in AI chatbots, which recognizes patterns and makes predictions, creating content from user prompts.

Topic	Definition
Large Language models	The “Large language Model (LLM)” is a type of AI that uses deep learning techniques and large data bases to understand, summarise, generate and predict new content.
Machine Learning	The term Machine Learning emerged as a subfield of Artificial Intelligence (AI) that focuses on developing algorithms and techniques to enable computer systems to learn and improve from data without being explicitly programmed.
Natural Language Processing/ Conversational AI	These AI systems are designed to interact with humans through Natural Language Processing (NLP), a subfield of computer science and AI that enables computers to understand, interpret, and generate human language.
Predictive AI	This type of AI uses historical data to make predictions about future events. It's commonly used in areas like finance for stock market forecasting, weather prediction, and customer behaviour analysis.
Robotic Process Automation	Robotic Process Automation (RPA) is a technology that uses software robots or "bots" to automate repetitive, rule-based tasks typically performed by humans, improving efficiency and accuracy in business processes.
AI Data Ethics	Systems will need to be developed ethically and clearly to ensure they address issues such as bias, discrimination, privacy and surveillance to avoid potential harm and maintain public trust.
Data Protection Impact Assessment	A Data Protection Impact Assessment (DPIA) is a process to identify and minimise data protection risks in a project.
Data Quality	Data Quality refers to the accuracy, completeness, reliability, and relevance of data, ensuring it is fit for its intended use.
Microsoft Co-pilot	Microsoft Copilot is an AI assistant designed to enhance productivity by providing intelligent, context-aware support and solutions across various tasks and applications.
Training Data	Training data is the dataset used to teach an AI model to recognise patterns, make decisions, and generate outputs based on the examples it has learned from.

4. Legislative and regulatory framework

This policy will also ensure compliance with all applicable UK legislation and statutory guidance in relation to use of AI including:

Legislation	Summary
UK General Data Protection Regulation 2016, Data Protection Act 2018, Data (Use and Access) Act 2025	Data protection legislation governs how personal data is processed, including by AI systems and provides statutory rights including the right to object to automated processing to challenge and prevent decisions made solely by automated systems that significantly affect them.
Equality Act 2010	Requires all AI systems to be fair and not discriminate against individuals based on protected characteristics.
Human Rights Act 1998	Protects fundamental rights and freedoms, including privacy and freedom of expression, which may be affected by AI use.
Freedom of Information Act (FOIA) 2000 and Environmental Information Regulations 2004	Under the FOIA/EIR, the Council has a duty to make information available to the public upon request, unless specific exemption(s) apply. It is also obliged to proactively and routinely publish information that has been frequently requested in the past in its Publication Scheme.
Contract, Copyright, and Intellectual Property Law	Contract Law in the UK governs the formation and enforcement of agreements between parties, Copyright Law protects the rights of creators over their original works, and Intellectual Property Law encompasses various legal protections for inventions, designs, trademarks, and trade secrets.
Statutory and recommended guidance	Guidance provided by the Information Commissioner's Office, HM Government Departments, the Local Government Association, and the National Cyber Security Centre.

5. Practical Requirement for Staff

- All AI use must be reviewed against the above legislation and guidance.
- A DPIA and EIA must be completed before any AI system is deployed or feature is enabled.
- Information Governance must be consulted at an early stage to ensure compliance.

6. Artificial Intelligence Principles

Middlesbrough Council adopts the following principles to ensure that AI is used lawfully, ethically, and responsibly. These are based on Central Government and adapted for the authority context, these are:

- We know what AI is and what its limitations are
- We use AI lawfully, ethically and responsibly
- We know how to use AI securely
- We have meaningful human control at the right stage
- We understand how to manage the AI life cycle
- We use the right tool for the job
- We are open and collaborative
- We work with commercial colleagues from the start
- we have the skills and expertise needed to implement and use AI
- We use these principles alongside our organisation's policies and have the right assurance in place.

7. Roles and Responsibilities

- **The Mayor and Elected Members of the Council** are democratically accountable for the way in which Middlesbrough Council discharges its functions. Information Governance (including Artificial Intelligence) sits within the portfolio of the Mayor.

- **The Chief Executive** has a duty to manage the discharge of the Council's different functions, including its legal responsibilities for effective information rights management. Oversight of the Council's information governance arrangements sit within the remit of the Corporate Affairs and Audit Committee.

- **The Head of ICT and Digital** will lead the Digital Strategy development and ensure planned use of AI within it adheres to this policy.

- **The Leadership Management Team** and **Directorate Management Teams** collectively and individually are the owners of the Council's 'information assets' and are responsible for the compliance of their services with legislation, associated codes of practice, guidance and this policy.

- **The Executive Director of Children's Services** and **Director of Adult Social Care and Health Integration** have been designated and registered by the Council as its 'Caldicott Guardians', the senior persons responsible for protecting the confidentiality of people's health and care information and making sure it is used properly.

- **The Head of Policy, Governance and Information** has been designated as the Council's Senior Information Risk Owner and they must foster a culture for protecting and using data, provide a focal point for managing information risks and incidents, and is concerned with the management of all information assets.
- **The Data Protection Officer's** role is to assist the Council to monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs), and act as a contact point for data subjects and the supervisory authority.
- **Technical Design Authority Board** is responsible for providing technical governance across all ICT and Digital projects. It will review and approve technical designs to ensure alignment with the Council's ICT and Digital Strategy, Information Strategy security standards, and architectural principles. The Board acts as an escalation point for technical risks, validates compliance with policies, and ensures proposed solutions are cost-effective, sustainable, and interoperable with existing systems.
- **Information Strategy Group** is responsible for overseeing implementation of the Council's agreed Information Strategy.
- **All staff, volunteers, and third parties** handling personal data on behalf of the Council must comply with legislation, the Council's AI Policy, and follow procedures and training. When using AI, users remain accountable for decisions, must review AI-generated answers, intervene if necessary, and identify any content produced by Generative AI when documenting or sharing it.

8. Supporting Policies

This Policy should be read in conjunction with the following other policies:

- Data Protection Policy
- Data Management policy
- Secure Working Policy
- Records Management Policy
- Public Information and Information Request Policy
- Equality Policy
- Impact Assessment Policy.

9. Procedure and Process

Middlesbrough Council will ensure that it maintains the required documentation, procedures, and processes in relation to its legal obligations and matters of good practice in relation to mitigation of risk including but not limited to:

Governance and Approval

- Technology Design Authority must review and approve all AI proposals.
- Functional system owners must consult Information Governance and update a DPIA before any AI functionality is purchased, enabled, or significantly changed.
- Significant AI projects must also be recorded in the AI Transparency Register and, where relevant, included in privacy notices and equality impact assessments.

Risk and Compliance

- Responsible procurement of AI, suppliers must demonstrate compliance.
- Appropriate training datasets.
- Business and decision-making process mapping.
- AI Transparency Register.
- Compliance audits (including contract monitoring).
- Fairness check assessments.
- Consultation with citizens and stakeholders.
- Performance monitoring.
- Privacy notices updated where AI is used.
- Data Protection Impact Assessments.
- Data protection by design and default.
- Equality Impact Assessments.
- Intellectual property and copyright compliance.
- Mandatory AI user training.

10. Monitoring and review arrangements

Compliance with this policy will be monitored by the Technical Design Authority within its oversight role.

This policy will be fully reviewed annually. The Head of ICT and Digital has the delegated authority to amend this policy to reflect emerging technologies and issues, following consultation with the Senior Information Risk Owner, Data Protection Officer and the Technical Design Authority.

11. Further Information

Additional guidance is available on **The Bridge**, Services, ICT, Artificial Intelligence. For queries about this policy, please contact the Head of ICT and Digital or the Data Protection Officer.

This page is intentionally left blank