

ABERDEEN CITY COUNCIL

COMMITTEE	Staff Governance
DATE	30 January 2023
EXEMPT	No
CONFIDENTIAL	No
REPORT TITLE	Use of Locating Systems in Vehicles and Devices Policy
REPORT NUMBER	CUS/23/041
DIRECTOR	Andy MacDonald – Director – Customer Services
CHIEF OFFICER	Isla Newcombe – Chief Officer – People and Organisational Development
REPORT AUTHOR	Kirsten Foley – Employee Relations and Wellbeing Manager
TERMS OF REFERENCE	2.5

1. PURPOSE OF REPORT

- 1.1 This report seeks approval for the Council's revised 'Use of Locating Systems in Vehicles and Devices Policy'.

2. RECOMMENDATION

That the Committee: -

- 2.1 approves the Council's revised 'Use of Locating Systems in Vehicles and Devices Policy' shown at Appendix 1;
- 2.2 notes the accompanying procedure and form to the policy at Appendix 2;
- 2.3 notes the engagement and consultation already undertaken with Trade Unions ; and
- 2.4 notes that the policy has been agreed by the Council's Risk Board and has been reviewed by the data protection team as part of the risk process.

3. CURRENT SITUATION

- 3.1 The Council's 'Use of Locating Systems in Vehicles and Devices Policy' has been in place since 2011 and was last reviewed in 2015, having been approved at the Finance, Policy, and Resources Committee on 15 September 2015. The policy was therefore due another review in accordance with the rolling programme of reviews of HR related policies.
- 3.2 The purpose of the policy is to ensure that the Council takes a consistent and corporate approach to the use and management of locating systems and to the use and management of data generated by such systems.

- 3.3 Locating systems use Global Positioning Systems (GPS) in real time or retrospectively and can identify the location of a vehicle or device they are fitted to. GPS units may be fitted to vehicles and devices such as radios and mobile devices e.g. handhelds, telephones, tablets.
- 3.4 The policy sets out the reasons the Council uses locating systems and when and how the data from those systems will or could be used. It aims to make this a transparent process to maintain trust and protect the interests of employees and the Council, while delivering efficient and effective services.
- 3.5 Locating systems are designed to be used for a variety of purposes such as health and safety, service performance management and resolving complaints, with these fully covered in the policy.
- 3.6 They are not used for monitoring the general whereabouts of employees aside for operational purposes as outlined in this policy. Before checking the location of an employee(s), the manager must have due cause within the reasons identified in this policy.
- 3.7 More employees are working 'smarter' through the application of flexible working options and many teams are adopting a mobile approach to service delivery with employees visiting sites or clients using handheld devices to complete their work, without having to return to the office. The Council is therefore committed to optimising the use of resources and technology, to improve the experience of both customers and staff.
- 3.8 Various teams in the Council now use locating systems and it is anticipated that more may introduce similar technology in the future or 'switch on' this capability in existing electronic devices.
- 3.9 The policy helps ensure that best use is made of the available technology and at the same time ensuring that it is used appropriately and for valid purposes, with the interests of employees protected.

Engagement and Consultation

- 3.10 A short life project group was set up to undertake the review of the policy. This group included representatives from services which make the most use of these systems, including Waste and Recycling, Roads, Building Services and City Wardens; Fleet Services and the Data Insights Team, in relation to the data protection/handling aspects of the policy.
- 3.11 In addition to the project group, engagement was undertaken with representative employees from Waste and Recycling, Roads, Building Services and City Wardens, in order to gain feedback from the frontline employees most closely involved with the systems.
- 3.12 Valuable feedback was also provided through the Trade Union engagement process, which included both engagement meetings and written feedback being provided by all unions. Union colleagues made a number of helpful suggestions which have been incorporated into the policy.

Policy Updates

- 3.13 It was identified from the review that most of the existing policy provisions were still relevant and should be carried over to the revised policy. There have not therefore been material changes to the policy in terms of accessing and using data from locating systems and in informing employees of same.
- 3.14 Most of the changes have related to necessary updating to accord with data access, handling, and retention requirements under the legislation; to reflect the current culture of the organisation; to explain the purpose of the policy more fully; and to detail the responsibilities of the various parties involved in the policy.
- 3.15 The specific changes made to the policy following the review are detailed in the table below:

Change made	Reason for change
Policy put into new corporate policy template format	To ensure a consistent approach to policy across the organisation
Procedural elements moved into separate document	To ensure a robust process is in place for recording any requests to access data
“Need for Policy” section updated	To clarify the purpose of the policy and the risks that it is mitigating
Scope section expanded	To give clarity on all systems, software and devices that are covered by the policy, and to reflect the culture of the Council through reference to the Guiding Principles
Addition of a “responsibilities” section	To ensure that all parties have a clear explanation of the expectations the policy places on them
Requirement for service level documentation procedures to be in place added	To ensure that GDPR compliant procedures are in place around the lifecycle management of any data generated by locating systems.
Requirement for Data Protection Impact Assessments to be undertaken	To ensure that in cases where major functional changes are proposed to existing systems, or it is planned to introduce a new system, appropriate impact assessments are undertaken prior to any changes being made.
References to legislation highlighted	To ensure that all relevant legislation is adhered to, including the General Data Protection Regulation (GDPR), the Data Protection Act 2018 and the Human Rights Act 1998.
Retention of Data and Records Section updated	To ensure compliance with the Records Retention and Disposal Schedule.

Reference to the strategic priority of Energy Transition and Net Zero added	To highlight how the policy may indirectly contribute to the strategic priority
Other minor updates to wording and terminology	

4. FINANCIAL IMPLICATIONS

4.1 There are no direct financial implications arising from the recommendations of this report.

5. LEGAL IMPLICATIONS

5.1 There are no direct legal implications arising from the recommendations of this report, however, having this Policy in place will assist the Council to comply with its statutory data protection duties.

6. ENVIRONMENTAL IMPLICATIONS

6.1 There are no direct environmental implications arising from the recommendations of this report.

7. RISK

Category	Risks	Primary Controls/Control Actions to achieve Target Risk Level	*Target Risk Level (L, M or H) *taking into account controls/control actions	*Does Target Risk Level Match Appetite Set?
Strategic Risk	No significant risks identified.	N/A	N/A	N/A
Compliance	There is a risk of non-compliance with Data Protection and Human Rights legislation through data from locating systems being accessed and used for inappropriate purposes.	Continuing to have this policy in place and communicating it across the organisation should help ensure that data from locating systems is only accessed and used in the circumstances defined under the policy, and that it is appropriately handled, helping avoid the risk of non-compliance with this legislation.	M	Yes

Operational	There is a risk of disruption to Council operations if industrial relations issues were to arise as a result of data from locating systems being accessed and used inappropriately.	Continuing to have this policy in place and communicating it across the organisation should help ensure that data from locating systems is only accessed and used in the circumstances defined under the policy, and that it is appropriately handled in accordance with this policy. This will help to reduce the chance of any such industrial relations issues arising which could disrupt Council operations.	M	Yes
Financial	There is a potential financial risk to the Council if a legal claim arose relating to data protection, discrimination, or constructive dismissal resulting from unlawful or unfair practices in connection with data from locating systems being accessed and used inappropriately.	Continuing to have this policy in place and communicating it across the organisation should help ensure that data from locating systems is accessed and used appropriately, hence helping to reduce the chance of any such legal claims against the Council arising.	M	Yes
Reputational	There is a potential reputational risk to the Council if a legal claim arose, as mentioned	Continuing to have this policy in place and communicating it across the organisation should help ensure that data from locating systems is accessed and used	M	Yes

	under 'Financial risk' above, which was publicised and resulted in damage to the standing of the Council.	appropriately, hence helping to reduce the chance of any such legal claims against the Council arising and any resulting reputational damage.		
Environment / Climate	No significant risks identified.	N/A	N/A	N/A

8. OUTCOMES

<u>COUNCIL DELIVERY PLAN 2022-2023</u>	
Impact of Report	
Aberdeen City Council Policy Statement <u>Working in Partnership for Aberdeen</u>	N/A
<u>Aberdeen City Local Outcome Improvement Plan</u>	
Prosperous Economy Stretch Outcomes	The Prosperous Economy theme in the LOIP makes mention of the importance of retaining talent and expertise in City organisations. This would include the Council. Having this revised policy in place, which should help ensure that data from locating systems is only accessed and used for appropriate purposes, may assist with employee relations in the organisation and with the retention of trained and valued employees. This would mean that they can continue in post and contribute to delivering effective services to citizens and businesses, indirectly contributing to the City's economy.
Prosperous People Stretch Outcomes	The Prosperous People theme in the LOIP indicates that all people in the City are entitled to feel safe, protected from harm and supported where necessary, which would include employees of the Council. Having this revised policy in place should help ensure that data from locating systems is accessed and used for appropriate purposes, (not for general monitoring) reducing the chances of complaints arising from staff and hence assisting with employee relations in the organisation. This may indirectly help promote employee mental health and

	wellbeing allowing staff to function both in employment and at home.
Regional and City Strategies	N/A

9. IMPACT ASSESSMENTS

Assessment	Outcome
Integrated Impact Assessment	An Integrated Impact Assessment has been compiled in respect of the revised policy and no negative impacts have been identified.
Data Protection Impact Assessment	
Other	N/A

10. BACKGROUND PAPERS

10.1 N/A

11. APPENDICES

- 11.1 Appendix 1 - Revised Use of Locating Systems in Vehicles and Devices Policy.
- 11.2 Appendix 2 - Process for Making a Specific Request to Access Recorded Data from a Locating System (including proforma).

12. REPORT AUTHOR CONTACT DETAILS

Name	Kirsten Foley
Title	Employee Relations and Wellbeing Manager
Email Address	Kfoley@aberdeencity.gov.uk
Tel	07789 914445

Use of Locating Systems in Vehicles and Devices Policy

**Approved by Committee on
?? with an implementation date of ??**
Sub-title – Calibri Bold 12pt (centred)

Document Control

Approval Date Calibri bold 12pt	- Calibri Regular12pt
Implementation Date	
Policy Number	Request from Assurance Team
Policy Author(s) and Owner	
Approval Authority	
Scheduled Review	
Date and Changes: This section should include details of the changes since the policy was last approved. November 2022 - This policy has been updated, put into the corporate policy template, and replaces the existing Use of Locating Systems in Vehicles and Devices Policy.	

Table of Contents

1	Why does the Council need this Policy?.....	11
2	Application and Scope Statement	11
3	Responsibilities	12
4	Supporting Procedures & Documentation	14
5	About this Policy	14
6	Risk.....	19
7	Environmental Considerations	20
8	Policy Performance	20
9	Design and Delivery	20
10	Housekeeping and Maintenance	21
11	Communication and Distribution	21
12	Information Management	21
13	Definitions and Understanding this Policy	21

1 Why does the Council need this Policy?

- 1.1 This policy is required to ensure that the Council takes a consistent and corporate approach to the use and management of locating systems, and to the use and management of data generated by such systems.
- 1.2 It sets out the reasons the Council uses locating systems and when and how the data from those systems will or could be used. It aims to make this a transparent process to maintain trust and protect the interests of employees and the Council, while delivering efficient and effective services.
- 1.3 The main risk the policy is mitigating against is the inappropriate or inadvertent use of data from a locating system, potentially resulting in an industrial relations issue and, or a legislative breach and reputational damage.
- 1.4 As a responsible employer the Council seeks to use the most up-to-date technology to deliver high quality services to customers whilst supporting and protecting employees in respect of their health, safety, and wellbeing.
- 1.5 More employees are working 'smarter' through the application of flexible working options and many Clusters are adopting a mobile approach to service delivery with employees visiting sites or clients using handheld devices to complete their work, without having to return to the office. The Council is committed to making best use of resources and technology, to improve both the customer and staff experience.
- 1.6 The ongoing development of technology means that it is possible to identify the location of a vehicle, plant, device and by default the user, by reference to associated Global Positioning Systems (GPS) in real time or retrospectively. GPS units may be fitted to vehicles, plant, and devices such as radios and mobile devices (e.g. handhelds, telephones, tablets).
- 1.7 Various Services in the Council use locating systems and it is anticipated that more may introduce similar technology in the future or 'switch on' this capability in existing electronic devices.
- 1.8 This policy helps ensure that best use is made of the available technology but at the same time that it is used for appropriate and valid purposes, with the interests of employees protected.

2 Application and Scope Statement

- 2.1 This policy applies to all employees and workers of the Council (including agency workers).
- 2.2 It applies to any systems, software or devices which have locating functionality enabled, and to any data generated by the use of any system, software or device with locating functionality, ensuring it is accessed and utilised for defined purposes only, in accordance with this policy. It is also concerned with ensuring that any specific requests for data access from locating systems are

done so in accordance with the agreed process, and that the data is handled in line with legislative requirements. The policy provisions are detailed under 5.91 to 5.95 below.

2.3 The policy accords with the use of all digital locating enabled devices in the organisation to help ensure effective asset management, health and safety, provision of service performance management information, resolution of complaints, assistance with employee relations and provision of financial data. It does not apply to staff's personal devices as detailed in the Bring Your Own Devices (BYOD) Policy.

2.4 It aligns with the Council's Guiding Principle of 'Valuing each other', confirming a commitment to ensuring everyone is treated with dignity and respect and supported by the organisation, also aligning with the principle of 'Trusting each other'.

3. Responsibilities

3.1 Chief Officers are responsible for the application of the policy within their service delivery remit, including ensuring:

- that all existing locating systems are used and managed in accordance with this policy.
- that any new locating systems under consideration are subject to an appropriate Data Protection Impact Assessment prior to adoption.
- the identification of authorised users.

3.2 The Chief Officer – Digital and Technology has overarching responsibility to determine the specification and implementation of all hardware and software digital solutions adopted for use within the Council and to secure the Council's digital infrastructure and information assets, including the application or removal of restrictions and tools to balance the needs of business against the risk of cyber attack.

3.3 The Council's Data Protection Officer is responsible for monitoring the Council's compliance with data protection law and providing advice on data protection across the organisation, including in relation to data associated with locating systems.

3.4 Service Managers have responsibility for applying this policy and its provisions including:

- Informing employees in their teams where a locating system is in operation or is to be introduced.
- Informing their employees about the scope and usage of any such locating system.
- Ensuring documented procedures are in place around the lifecycle management of any data generated by location systems in use within their area.
- Ensuring their employees know of this policy and where it can be accessed.

- Ensuring that any specific requests for data access from a locating system are undertaken in accordance with the agreed process referred to in this policy, including obtaining the necessary authorisation.
- Ensuring that any data they are authorised to access from a locating system is handled in accordance with this policy and legislative requirements.

3.5 Information Asset Owners, (who may also be Service Managers), have a responsibility to:

- Manage information assets, including locating systems, throughout their lifecycle.
- Understand the risks associated with data handling and processing and provide assurance.
- Foster a culture where information is valued, respected, and protected.
- Ensure that information assets, including locating systems, are used for the public good.

3.6 Authorised Users of locating systems have responsibility to:

- Observe strict confidentiality in the handling of data from a locating system in accordance with this policy.
- To only access data they are authorised to view and report on.
- To only access and use data for purposes connected with their job role.

3.7 Employees have a responsibility to:

- Familiarise themselves with the contents of this policy.
- Co-operate with management in respect of any investigation arising out of the use of data from a locating system.

3.8 In the event of information being required from any locating system as part of an investigation concerning the performance or conduct of an employee, the Investigating Officer has a responsibility to obtain written authority from a Service Manager, Chief Officer, or Director to access the requested information. See paragraph 5.93 below.

3.9 A breach or misuse of this policy may result in the potential use of a corporate procedure e.g. disciplinary procedure.

3.10 Non-compliance with this policy should be reported to the employee's line manager, senior manager, or People and Organisational Development, to allow the appropriate next steps to be determined.

3.11 Any feedback on the policy or suggestions for improvement can be communicated to the Chief Officer – People and Organisational Development, or the Employee Relations and Wellbeing Manager, and this will be taken into account as part of the regular review of this policy.

4 Supporting Procedures & Documentation

4.1 The policy links directly to the Digital Devices Vehicles and Plant Procedure and the City Warden and Community Safety Tracking Devices Operating Procedure.

4.2 This policy also links to:

- Managing Discipline policy, and accompanying procedure and guidance
- Corporate Information Policy and supporting Corporate Information Handbook of procedures
- Council's Guiding Principles

5 About this Policy

5.1 The policy is not creating any specific regulations or requirements other than what is stated under Core Principles as below. The policy provisions are detailed below under paragraphs 5.91 to 5.95.

5.2 It is intended that the policy will be followed in all circumstances to ensure that data from locating systems is used appropriately and for the benefit of the organisation so that the investment in this new technology is realised, but at the same time ensuring its use is in accordance with the provisions of this policy, so that employee interests are also protected.

Core Principles

5.3 The primary uses of any locating system used by the Council are for employee health and safety, to manage service performance and in connection with any complaints received.

5.4 Locating systems will not be used for monitoring the general whereabouts of employees aside for operational purposes as outlined in this policy. Before checking the location of an employee(s), the manager must have due cause within the reasons identified in this policy.

5.5 Where a serious (not minor) performance or conduct issue arises with an employee, a Service Manager, or above, may give authority to request access from the relevant Information Asset Owner to locating system data and use this in respect of the particular issue. See further details below under Policy Provisions and in the accompanying process.

5.6 Clusters will ensure that all relevant employees are informed about the scope and usage of any locating systems.

5.7 In the event of any major functional changes to an existing system or plans to use a new locating system, engagement will take place with the trade unions and relevant employees prior to it being introduced.

5.8 In the event of any major functional changes to an existing system or plans to use a new locating system, the Council shall undertake a Data Protection Impact Assessment prior to adoption.

5.9 When using locating systems, the Council will adhere to the requirements of the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018, and the provisions of the Human Rights Act 1998.

POLICY PROVISIONS

5.10 Informing Employees

Where a locating system is in operation, or is to be introduced, there is a requirement of Clusters to ensure that all relevant employees are informed about the scope and usage of the system(s). This includes key fobs or tachographs (these provide links between GPS data and the personal information of an employee) in the equipment or vehicle the employee may use. Employees shall be informed of the existence of this policy and its provisions in respect of how it applies to their role and of how to access it. New employees will be informed of the above as part of the induction process.

5.11 Information Use

The primary uses of information recorded by any form of locating system is in relation to the health and safety (e.g. Lone Workers or Out of Hours Workers) to help ensure a safe and healthy work environment for employees, in relation to managing service performance (e.g. monitoring utilisation and efficiency or measuring compliance with legislation requirements) and in connection with any complaints from the public.

In addition, there may be occasions where the Council requires to access specific information concerning the performance and/or conduct of an employee where a management concern has arisen. Although this is not one of the main uses of the information recorded by a locating system it may be used for such a purpose. Where a specific check(s) is to be carried out, employees shall be directly informed of this unless to do so would be likely to prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.

The table below shows the purpose of the information recorded by a locating system and what this information will/could be used for.

<i>Purpose - Type of Information</i>	<i>How this information may be used</i>
<p>Health and Safety</p> <ul style="list-style-type: none"> ○ Lone working ○ Locating employees when other forms of communication are lost ○ Breakdowns ○ Vehicle or equipment theft ○ Risk assessments ○ Accidents/Incidents 	<p>Enables a Cluster to track the location of a vehicle and/or employee(s) where they have become un-contactable during their duties in working hours, which could involve using real time information. Some devices may also have the function of a ‘panic button’ that can be used for health and safety purposes.</p> <p>Enables the location of the vehicle to be tracked in the event of a Council vehicle or equipment being stolen.</p>
<p>Service Performance</p> <p>Management Information</p> <ul style="list-style-type: none"> ○ Historic record of service performance ○ Vehicle usage and efficient routing ○ Target and divert resources to meet customer need ○ Operational constraints ○ Cost reduction ○ Carbon management planning ○ Vehicle usage /carbon footprint information. 	<p>Enables a Cluster to review management information reports retrospectively or real time technical, financial, and administrative data such as distances travelled, driving speeds, driving times, lost time (due to traffic) etc. This management information can be used to aid and improve service performance.</p> <p>Enables a Cluster to manage and divert resources to meet customer needs and complete daily tasks, which could involve using real time information.</p>
<p>Resolving Complaints</p> <ul style="list-style-type: none"> ○ Details/information relating to a complaint received 	<p>Enables a Cluster to review factual information relating to a complaint from a service user/member of the public, to assist in the provision of a response to the individual and in the resolution of the particular issue.</p>
<p>Employee Information</p> <ul style="list-style-type: none"> ○ As part of an investigation in relation to a specific performance and/or conduct issue. 	<p>Enables a Cluster to review factual information relating to an employee’s location at a date(s) and/or time(s) (or an approximate timeframe). This would be in relation to a performance or conduct investigation.</p>

Tax Requirement <ul style="list-style-type: none"> ○ Record of vehicle use 	Enables a Cluster to provide factual information to demonstrate that a vehicle has not been used for personal purposes in connection with personal tax liabilities.

5.12 Access to the Information

- **Cluster Management**

Locating systems will differ across Clusters and as a result each will have different access requirements and information and reporting needs. Therefore, it is the responsibility of each Cluster to have local data management arrangements in place, including details of authorised users of the system in the Cluster. Some Clusters will access data on a 'real time' basis for health and safety purposes or to ensure that resources are effectively deployed on a daily basis. In addition, retrospective information may be used for monitoring and analytical purposes over a longer period.

Where information is extracted from a system for the purpose of improving service delivery, it will be anonymised to ensure that there is no link to an employee in relation to specific records.

Where an issue or concern within the principles and provisions of this policy is raised and the system has the recorded data that relates to the issue or concern, access to the data will be via a written request from the Officer seeking to access the data (see accompanying process). This request must be submitted for authorisation by a Service Manager, Chief Officer, or Director explaining the reason(s) the data is required, which must be consistent with the principles and provisions of this policy. This authority will only be given in relation to information that pertains to the area of concern and the information request must be in relation to a date(s) and/or time(s) (or an approximate timeframe) and within the principles and provisions of this policy.

- **By an Investigating Officer**

In the event of information being required from any locating system as part of an investigation concerning the performance or conduct of an employee, the Investigating Officer must have written authority from a Service Manager, Chief Officer, or Director to access the requested information. This authority will only be given in relation to information that pertains to the investigation and the information request must be in relation to a date(s) and/or time(s) (or an approximate timeframe) and within the principles and provisions of this policy.

Each Cluster will retain records of the date upon which information was provided from a locating system in relation to an employee's performance or conduct and details of the person who accessed the system.

- **Subject Access Requests for Information**

Under Data Protection legislation, employees have the right of a subject access request in relation to their own personal data. Such requests must be referred to the Council's Access to Information Team and be handled in accordance with relevant Council policy and procedures.

- **Third Parties**

Information collected through any locating system, in relation to an employee, will not generally be disclosed to a third party (this includes other employees, any freedom of information requests or requests from other public authorities), without the prior knowledge and consent of the employee concerned, except where such release is permitted or required by law. All requests for personal data from third parties must be referred to the Council's Access to Information Team and be handled in accordance with relevant Council policy and procedure.

5.13 Storage of Data and Records

In the event that information is extracted from a system and produced in an alternative format (e.g. paper, digital file) the records will be stored securely and will only be accessible to those with authority to access the data, in the particular Cluster.

5.14 Retention of Data and Records

Information collected by a locating system will not normally be retained for longer than 6 months. All new systems which capture location data should have the functionality to automate the deletion of data in accordance with the Council's retention and disposal schedule.

Where information collected by a locating system is required for the purposes of an investigation, it will form part of the investigation record, and will be retained in accordance with the relevant retention period outlined in the Council's retention and disposal schedule. Investigation records will

be managed in accordance with the Council's Corporate Information Policy and Supporting Procedures.

In the event that a record is, or seems likely to be, required in connection with court or legal proceedings, then advice should be sought from the Council's Data Protection Officer.

All records will be disposed of in accordance with the Council's Records Retention & Disposal Schedule.

6 Risk

6.1 The following identified risks will be mitigated against through having this policy in place.

- Compliance - the main purpose of the policy is to ensure that data from locating systems is only accessed and used in the circumstances defined under the policy, and that it is appropriately handled, helping avoid the risk of non-compliance with Data Protection and Human Rights legislation.
- Operational – where data from locating systems is accessed and used appropriately, in accordance with this policy, this will reduce the chance of any industrial relations issues arising which could disrupt Council operations.
- Financial – the policy should contribute to the avoidance of claims against the Council relating to data protection, discrimination, or constructive dismissal resulting from unlawful or unfair practices, which can be costly.
- Reputational - if the policy is applied correctly claims such as those detailed in the bullet point above will be avoided, which will prevent any reputational damage occurring in relation to a legislative or unfair practice breach.

6.2 There have been no unintended effects, consequences and risks identified resulting from the introduction of the policy. This will continue to be monitored as the policy is applied.

6.3 The risks identified will be managed and mitigated through application of the policy across the Council. This will be undertaken by ensuring the policy is readily available to all staff and that support is provided from People and Organisational Development in the interpretation of the policy, where required.

6.4 Monitoring will be undertaken of any feedback from stakeholders or others in relation to the identified risks and appropriate action taken if any concerns arise.

6.5 The policy should also support the organisation's 'PREVENT' obligations as part of the 'CONTEST' framework by helping to maintain employee trust in the organisation by ensuring that data from locating systems is accessed and used in accordance with the policy. This should

help to maintain staff health and wellbeing, reduce their vulnerability and in turn make them less susceptible to radicalization and being drawn into terrorist organisations.

7 Environmental Considerations

- 7.1 Hardcopy printouts of data from a locating system will only be undertaken where appropriate, to minimise usage of paper, with digital records to be utilised wherever possible.
- 7.2 The policy should indirectly contribute to the Council's Strategic Priority of Energy Transition and Net Zero, with the uses of data from locating systems including vehicle utilisation, efficient routing, carbon management planning and identification of any carbon footprint.

8 Policy Performance

- 8.1 One of the main factors determining the effectiveness of the policy will be adherence to it by Clusters who make use of locating systems, with the information and data only being used in accordance with the reasons detailed in this policy, and with any specific requests for access being made in line with the accompanying process. In addition, adherence to the retention and storage of the data provisions on locating systems will be another factor determining its effectiveness, with legislative requirements requiring to be met.
- 8.2 The effectiveness of the policy will be measured by monitoring any complaints received from employees, trade unions, or others, in relation to the access or use of data from a locating system. Feedback from users to whom the policy applies will also be monitored to check that it is operating as intended, and if it is not, to consider any necessary changes.
- 8.3 The Chief Officer – People and Organisational Development will decide where and when data is reported on the effectiveness of the policy, also ensuring that confidentiality is maintained.

9 Design and Delivery

- 9.1 The policy links to the 'Workforce Design' principle of the Target Operating Model of the Council in that it is concerned with organisational culture and promotion of fairness in the workplace, in connection with the use of locating systems. The application of the policy should help ensure alignment with this principle. It also links to the Council's Guiding Principles of valuing and supporting staff and trusting one another.
- 9.2 The policy also aligns with the 'Prosperous People' theme in the Local Outcome Improvement Plan (LOIP) which indicates that all people in the City are entitled to live in a manner in which they feel safe and protected from harm and supported where necessary. All citizens are equally entitled to enjoy these aspirations, including employees of the Council. Having a policy of this

type in place where locating systems data is only used for defined purposes, including in relation to staff health and safety, should assist with employee wellbeing, with it being clear that it is not being used for general monitoring of their whereabouts. This should indirectly contribute to a safe and healthy workplace for all.

- 9.3 The policy should indirectly contribute to the Council's Strategic Priority of Energy Transition and Net Zero, with the uses of data from locating systems including vehicle utilisation, efficient routing, carbon management planning and identification of any carbon footprint.
- 9.4 The provisions detailed under paragraphs 5.94 and 5.95 above, covering storage and retention of data will help ensure alignment of the policy to support the Council's statutory obligations in relation to data protection.

10 Housekeeping and Maintenance

- 10.1 The policy will be reviewed annually, and any necessary updates made to it. It replaces the existing Locating Systems in Vehicles and Devices policy.

11 Communication and Distribution

- 11.1 This policy and supporting documentation will be shared directly with the Extended Corporate Management Team to enable communication and distribution in accordance with the responsibilities set out in section 4 above.
- 11.2 The policy and documentation will be available for review on the organisation's shared areas on the intranet. Any future updates to the policy will also be appropriately communicated.

12 Information Management

- 12.1 Information generated by the application of the policy will be managed in accordance with the Council's Corporate Information Policy and supporting Procedures.

13 Definitions and Understanding this Policy

- 13.1 Locating systems – are systems that use Global Positioning Systems (GPS) in real time or retrospectively, that can identify the location of a vehicle or device they are fitted to. The systems are designed to be used for a variety of purposes such as health and safety, service

Please provide details of what specific information is requested including relevant date(s) and/or time(s) (or an approximate timeframe) and locating system or device:

Signature: Date:

Authorised? Yes/No	
Any comments in relation to the decision: If the decision is 'No', please provide explanation:	

Name of authoriser:

Job Title of authoriser:
(Authoriser must be a Service Manager, Chief Officer, or Director)

Signature of authoriser: Date:

Note: Once this form has been fully completed, the Service Manager, Chief Officer, or Director, whichever applies, will notify the Officer who made the request of their decision on whether access to the recorded data on a locating system is authorised. This form will then be passed to the HR and Payroll Service Centre for filing.