PENZANCE COUNCIL – 16 MARCH 2026

REPORT FOR DECISION

AMENDMENT TO CALENDAR OF MEETINGS – DATE OF ANNUAL COUNCIL MEETING

Our Culture	Our Decision Making	Our Environment	Our Money	Our People	Our Places	Our Resilience & Wellbeing
	✓			✓		

Recommendation:

An amendment be made to the Calendar of Meetings to allow the Annual Council meeting to be held on Monday 18 May 2026.

Background:

Officers have sought to replicate the success of the 2025 Mayor's Christmas Celebration by holding this year's Annual Council meeting and reception in the same venue. However, the venue is unavailable on the date approved by the Council, Tuesday 12 May 2026, but is available on Monday 18 May 2026.

Members have been consulted informally, and no objections have been raised, and it is therefore recommended that the Calendar of Meetings be amended and the Annual Council meeting rearranged to take place on Monday 18 May 2026.

Elliot Ridington
Democratic Services and Governance Officer

PENZANCE COUNCIL 16 MARCH 2026

REPORT FOR DECISION

GENERAL DATA PROTECTION REGULATIONS - COMPLIANCE POLICIES

Our Culture	Our Decision Making	Our Environment	Our Money	Our People	Our Places	Our Resilience & Wellbeing
	✓			✓		✓

RECOMMENDATION

1. The IT, Data Security and Device Policy, as set out at Appendix 1 to this report, be approved and the document be adopted, superseding both the existing Mobile Phone and Laptop Policy and the existing Data Protection Policy.

2. The Data Breach Policy, as set out at Appendix 2 to this report, be approved and the document be adopted.

3. The Data Erasure Policy, as set out at Appendix 3 to this report, be approved and the document be adopted.

4. The revised Data Retention Policy, as set out using tracked changes at Appendix 4 to this report, be approved and the document be adopted.

5. The Subject Access Request Policy, as set out at Appendix 5 to this report, be approved and the document be adopted.

6. The Privacy Notice, as set out at Appendix 6 to this report, be approved and the document be adopted.

BACKGROUND

A review of the Council's data protection arrangements has been undertaken to ensure compliance with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018

This review was also necessary in order to support the Council's compliance with Assertion 10 of the Annual Governance Statement, which requires the Council to confirm that appropriate arrangements are in place for data security and cyber security management.

The review identified that several existing policies required updating, consolidation or replacement to ensure the Council has a clear, modern and legally compliant framework for managing personal data.

The attached policies establish procedures for:

- the secure use of IT systems and devices
- the management of personal data
- responding to data breaches
- responding to Subject Access Requests
- lawful retention and deletion of records
- transparency regarding how personal data is used

Together these policies form a coherent data protection framework to support lawful and secure management of personal data across the Council's activities.

Policy Name	**Notes**
IT, Data Security and Device Policy	Sets out rules for the safe use of Council IT systems, devices and information, replacing older separate policies.
Data Breach Policy	Provides a procedure for identifying, reporting and managing data breaches in line with ICO requirements.
Data Erasure Policy	Establishes how the Council responds to requests for deletion of personal data and ensures data is not retained longer than necessary.

Data Retention Policy	Sets out how long different types of Council records must be kept and when they should be securely destroyed.
Subject Access Request (SAR) Policy	Provides a procedure for responding to requests from individuals seeking access to their personal data.
Privacy Notice	Explains how the Council collects, uses and protects personal data in accordance with legal requirements.

Appendix 1 - IT, Data Security and Device Policy
Appendix 2 - Data Breach Policy
Appendix 3 - Data Erasure Policy
Appendix 4 - Data Retention Policy
Appendix 5 - SAR Policy
Appendix 6 - Privacy Notice

Cal Bagshaw
Corporate Services Manager

PENZANCE COUNCIL

IT, Data Security and Device policy.

CURRENT POLICY STATUS

Version:	1	Approving Body:	Council
Date:	16/3/2026	Date of Approval:	
Responsible Officer:	Town Clerk	Minute Reference:	
Overview Committee:	F&GP	Review Date:	16/3/2027

VERSION HISTORY

DATE	VERSION	AUTHOR/EDITOR	COMMENTS
16/3/2026	1	Cal Bagshaw CSM	New Policy

REVIEW RECORD

DATE	TYPE OF REVIEW	COMPLETED BY

This data security and bring your own device policy sets out the procedures Penzance Council have put in place to maintain the security of personal data and other data within our authority.

Penzance Town Council is a council in England.
Its contact details are:

Penzance Council,
Penlee Centre, Penlee Park, Penzance, TR18 4HE

Penzance Town Council is a data controller for personal data as defined by all applicable data protection and privacy laws including, but not limited to the retained EU law version of the General Data Protection Regulation ((EU)

2016/679) (the “UK GDPR”), as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, the Data Protection Act 2018; the Privacy and Electronic Communications Regulations 2003 as amended, and any successor legislation (the “Data Protection Legislation”).

This policy is binding on all officers, Members and volunteers (“User" or "Users”) of Penzance Town Council (“The Authority”) in order to protect Personal or other Data ("Personal Data" or "Data”) processed by the authority.

It applies to all organised filing systems be they computer based, paper based or any other such method of organising information which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis (“Filing Systems”).

Person Responsible

The Town Clerk is responsible for the ongoing compliance monitoring of this and other policies that are designed to achieve compliance with the Data Protection Legislation. (“the person responsible for data protection”).

No user within the authority shall deviate from this policy without written authorisation from the person responsible for data protection.

Acceptable Use

Data shall only be used within the authority for the purposes of the authority.

Data shall not be shared with third parties or other data controllers without a data sharing agreement having been finalised and signed by the person responsible for data protection.

Only data processors that have contracts with the authority that have been authorised by the person responsible for data protection shall be used.

Users processing data on behalf of the authority are reminded of the need to keep proper records in accordance with this and other policies designed to maintain compliance with the data protection legislation and the Freedom of Information Act.

Passwords

Users processing data on behalf of the authority on systems which require passwords shall use a password that:

- Is sufficiently complex and is made up of at least three random unconnected words.
- Is not used for other logins be they personal or professional.
- Is not disclosed to anyone nor written down.

Device password must be changed at least every 90 days.

Passwords must not be shared amongst the authority's users. If a user has a legitimate need for data that they cannot access with their own password then the person responsible for data protection shall be advised so that access levels may be changed if appropriate.

Users should be aware that no one will ever ask a user for their password. Any request for a password to be disclosed should be reported to the person responsible for data protection immediately.

Where multi factor authentication is available it must be used.

Multi factor authentication codes must not be disclosed to others or shared amongst the authority's users.

Users should be aware that no one will ever ask a user for a multifactor authentication code. Any request for a multifactor authentication code to be disclosed should be reported to the person responsible for data protection immediately.

Email

The authority does not allow users to process the authority's data using any email account other than that issued to them on the Penzance-tc.gov.uk domain or Penleehouse.org.uk domain

The authority does allow users to access email accounts provided by the authority using their own personally owned computers, laptops, or other mobile devices but the authority's data must remain within the authority's email system, attachments or other data must not be downloaded onto the device in question.

Social Media and Instant Messaging

The authority's data shall not be uploaded, posted or otherwise transferred to social media (including but not limited to Facebook, Twitter, Instagram, TikTok, YouTube) without the authorisation of the person responsible for data protection.

The authority's data shall not be uploaded, posted or otherwise transferred to instant messaging or collaboration services (including but not limited to Whatsapp, Teams, Skype, Facebook Messenger, Slack, Google Workspace) without the authorisation of the person responsible for data protection.

Social media, instant messaging and collaboration services that are authorised for use in the authority are listed in appendix A.

Physical Security

Servers shall be located in locked cabinets.

Devices shall not be left unattended without the screen being locked or the user logged out.

Paper files shall be kept in locked filing cabinets.

Documents no longer required shall be disposed of via secure means such as cross cut shredding or commercial document destruction.

Where documents are disposed of by commercial document destruction they shall be disposed of securely and a certificate of destruction obtained

System Security

Users of the authority's data shall be granted the appropriate level of access to cloud or computer systems to allow them to undertake their duties.

Routine working with administrator rights is not allowed, this is reserved for the use of the Council’s appointed IT provider only

Computer files and records shall be kept within the Council's server or cloud storage system.

USB sticks and other removable media shall not be used on the authority's computer

system unless the particular device and usage case is specifically approved by the person responsible for data protection.

Storage media on servers shall be encrypted.

Servers shall be backed up using a minimum 3-2-1 strategy: (3 copies of the data., On 2 different media types, with 1 backup off site.)

Cloud servers shall be backed up by the cloud service provider in a way that is not le ss robust than a 3-2-1 strategy.

Backups shall be subject to twice yearly recovery testing to ensure that they are fit for purpose.

Software including operating systems shall be regularly kept up to date and patched with the latest security updates from its developers.

WiFi networks shall have a minimum WPA2 encryption standard if they are used to tr ansmit data.

Public WiFi provided by the auhtority shall be firewalled in such a way that the authority's data is segregated from it.

Regular penetration testing at least 2 times a year shall be undertaken on all firewalls and computer network security systems.

Suitable anti virus software and anti malware software shall be used on all of the authority's computers, laptops or other mobile devices.

The auhtority does not allow users to join their own personally owned computers, laptops, or other mobile devices to the auhtority's computer network used for process ing data unless authorised by the person responsible for data protection.

Erasure

When electronic documents, files or records are no longer required they shall be deleted in such a way as to put the data beyond use.
Data will be retained and deleted in line with the Council's Data Retention policy

Data will be deemed to be put beyond use if:

1. The data is not able to be used to inform any decision in respect of any individual or in a manner that affects the individual in any way, and
2. The authority does not give any other authority access to the data, and

3. The authority surrounds the personal data with appropriate technical and auhtorityal security, and
4. The authority commits to permanent deletion of the information if, or when, this becomes possible.

Breaches

Any suspected breach of the confidentiality integrity or availability of personal data within our authority shall be immediately – that is within 1 hour wherever possible and never any later than 4pm of the same working day - notified in writing to the person responsible for data protection.

Breaches of the confidentiality, integrity or availability of personal data within the authority shall be investigated immediately by the person responsible for data protection and a determination made as to the level of risk of data being breached, the number of individuals involved, the severity of any breach and if the Information Commissioner's Office should be notified. This investigation must take a maximum of 72 hours from the first discovery of the breach.

No user should try to rectify a breach without first informing and getting authorisation from the person responsible for data protection.

Cyber Security Training

All users with access to Council systems or personal data must complete approved cyber security training on induction and at least annually thereafter.

The Council will maintain records of completion and may suspend system access where mandatory training is not completed.

Care of Issued Devices

All users issued with Council devices are responsible for their safe use, secure storage and reasonable care. Devices must be protected from loss, theft, damage and unauthorised access.

Loss, theft or damage must be reported immediately. Failure to take reasonable care may result in withdrawal of the device and may be addressed under the Council's disciplinary procedures where appropriate.

Updates to this policy

This policy shall be reviewed annually by the person responsible for data protection.

This policy shall be reviewed if Penzance Town Council makes changes to the authority's Privacy Notice or if there are changes to how the authority processes data or the data protection legislation changes.

This policy was last updated on 16/3/2026

Implementation

This policy takes effect from 16/3/26 and is not retroactive.

Appendix A - Social media, instant messaging and collaboration services that are authorised for use in the authority

Company	Product	Processor or Controller	Reason
Meta Platforms Inc.	Facebook page	Controller (joint)	Community engagement and information Authority controls page content but Facebook determines platform data processing
Meta Platforms Inc.	Instagram	Controller (joint)	Community engagement and information Authority controls page content but Facebook determines platform data processing
Microsoft	Teams	Processor	Collaberation platform for internal communication in text and video
Meta Platforms Inc.	Officer Whatsapp accounts	Processor	Messaging platform used for communication;

PENZANCE COUNCIL

Data Breach policy

CURRENT POLICY STATUS

Version:	1	Approving Body:	Council
Date:	16/3/2026	Date of Approval:	
Responsible Officer:	Town Clerk	Minute Reference:	
Overview Committee:	F&GP	Review Date:	16/3/2027

VERSION HISTORY

DATE	VERSION	AUTHOR/EDITOR	COMMENTS
16/3/2026	1	Cal Bagshaw CSM	New Policy

REVIEW RECORD

DATE	TYPE OF REVIEW	COMPLETED BY

This personal data breach policy sets out the procedures Penzance Town Council has put in place to deal with a breach of the confidentiality, integrity or availability of personal data within the authority.

Penzance Town Council is a council in England. The Authority's contact details are:

Penzance Town Council,
Penlee Centre, Penlee Park, Penzance, TR18 4HE

The Authority is data controller for personal data as defined by all applicable data protection and privacy laws, including, but not limited to, the retained EU law version of the General Data Protection on Regulation ((EU) 2016/679) (the "UK GDPR). As it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue

of section 3 of the European Union (Withdrawal) Act 2018, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 as amended, and any successor legislation (the “Data Protection Legislation”).

This policy is binding on all employees, Members and volunteers (“User" or "Users”) of Penzance Town Council (“The Authority”) in order to protect Personal or other Dat a ("Personal Data" or "Data”) processed by The Authority.

It applies to all organised filing systems be they computer based, paper based or any other such method of organising information which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or ge ographical basis (“Filing Systems”).

Definitions

“Personal data” means any information relating to an identified or identifiable individual (“data subject”); an identifiable individual is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

Personal data will typically contain information about the individual or their activities.

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, data. This includes breaches that are the result of both accidental and deliberate causes.

Personal Data breaches can include but are not limited to:

- Access by an unauthorised third party.
- Deliberate or accidental action (or inaction) by a controller or processor.
- Sending personal data to an incorrect recipient.
- Computing devices containing personal data being lost or stolen.
- Paper files containing personal data being lost or stolen.
- Alteration of personal data without permission, and
- Loss of availability of personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data.

There will be a personal data breach whenever any personal data is accidentally lost, destroyed, corrupted or disclosed or if someone accesses the data or passes it on

without proper authorisation or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

Who is responsible for managing personal data breaches

The Town Clerk is responsible for the ongoing compliance monitoring of this and other policies that are designed to achieve compliance with the Data Protection Legislation. ("the person responsible for data protection").

No user within the authority shall deviate from this policy without written authorisation from the person responsible for data protection.

Time limits

Not all personal data breaches are reportable to the Information Commissioner's Office ("ICO") but those that are must be reported within 72 hours of 'becoming aware' of a breach.

The 72 hour time frame is irrespective of bank holidays or weekends.

Users who suspect there has been a breach must notify in writing the person responsible for data protection immediately – that is within 1 hour wherever possible and never any later than 4pm of the same working day.

Investigation

The person responsible for data protection shall undertake an investigation of a suspected personal data breach to ascertain the circumstances of the breach and whether or not the breach was a result of human error or a systemic issue.

The investigation should consider if a recurrence can be prevented.

If human error is the cause of the personal data breach, the investigation should consider if:

- Data protection induction and refresher training for users is adequate.
- Support and supervising of users in their role is adequate.
- Policies and procedures require updating.

If the breach was caused by a systemic issue, the investigation should consider if:

- Access levels are fit for purpose.

- If a wider system audit should be undertaken.

- Do technical and organisational measures to maintain data security need to be reviewed.
- Do additional technical and organisational measures to maintain data security need to be implemented?

Notifying the ICO

The ICO must be notified of breaches where there is a likelihood of risk to people's rights and freedoms.

If a risk is likely, the person responsible for data protection must notify the ICO within 72 hours of 'becoming aware' of a breach.

If a risk is unlikely, there is no requirement to report it, but a voluntary report may still be made if the person responsible for data protection so decides.

If a breach has occurred and it has been decided not to report to the ICO then the decision and reasons shall be documented by the person responsible for data protection in the Penzance Town Council breach register.

If a breach has occurred and it has been reported to the ICO then the decision and reasons shall be documented by the person responsible for data protection in the Penzance Town Council breach register.

Telling data subjects

If there has been a personal data breach where there is a likelihood of risk to people's rights and freedoms the person responsible for data protection should contact those individuals affected and:

Describe in clear and plain language, the nature of the personal data breach and at least:

- The name and contact details of the person responsible for data protection as a point where more information can be obtained.
- A description of the likely consequences of the personal data Breach.
- A description of the measures taken or proposed to deal with the personal dat a breach and, where appropriate, a description of the measures taken to mitig ate any possible adverse effects.

If possible, the person responsible for data protection should give specific and clear advice to individuals on the steps they can take to protect themselves, and what Penzance Town Council is willing to do to help them. Advice could include but is not limited to:

- A password reset.
- Advising individuals to use strong, unique passwords.
- Telling individuals to look out for phishing emails or fraudulent activity on their accounts.

Users Role in Personal Data Breach

Users must notify in writing the person responsible for data protection immediately and in any case within 1 hour of any actual or suspected personal data breach.

No user should try to rectify a breach without first informing and getting authorisation from the person responsible for data protection.

Users must provide all timely assistance to the person responsible for data protection in the course of their investigation.

Obstruction of the investigation will be addressed via the relevant disciplinary procedure.

Updates to this policy

This policy shall be reviewed annually by the person responsible for data protection.

This policy shall be reviewed if Penzance Town Council makes changes to the authority's Privacy Notice or if there are changes to how the authority processes data or the data protection legislation changes.

This policy was last updated on 16/3/2026.

Implementation

This policy takes effect from 16/3/2026 and is not retroactive.

PENZANCE COUNCIL

Personal Data Erasure Policy

CURRENT POLICY STATUS

Version:	1	Approving Body:	Council
Date:	16/3/2026	Date of Approval:	
Responsible Officer:	Town Clerk	Minute Reference:	
Overview Committee:	F&GP	Review Date:	16/3/2027

VERSION HISTORY

DATE	VERSION	AUTHOR/EDITOR	COMMENTS
16/3/2026	1	Cal Bagshaw CSM	New Policy

REVIEW RECORD

DATE	TYPE OF REVIEW	COMPLETED BY

This personal data erasure policy sets out the procedures Penzance Town Council has put in place to deal with the erasure of personal data within The Authority.

Penzance Town Council is a council in England. The Authority's contact details are:

Penzance Council,
Penlee Centre, Penlee Park, Penzance, TR18 4HE

The authority is data controller for personal data as defined by all applicable data protection and privacy laws. Including, but not limited to, the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (the "UK GDPR), as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of

section 3 of the European Union (Withdrawal) Act 2018, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 as amended, and any successor legislation (the “Data Protection Legislation).

This policy is binding on all employees, Members and volunteers (“User" or "Users”) of Penzance Town Council (“The Authority”) to protect Personal or other Data ("Pers onal Data" or "Data”) processed by The Authority.

It applies to all organised filing systems be they computer based, paper based or any other such method of organising information which is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis (“Filing Systems”).

Definition of Personal Data

“Personal data” means any information relating to an identified or identifiable individual (“data subject”); an identifiable individual is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to more factors specific to the physical, physiological, generic, mental, economic, cultural, or social identity of that individual.

Personal data will typically contain information about the individual or their activities.

Who is Responsible for Managing Erasure of Personal Data

The Town Clerk is responsible for the ongoing compliance monitoring of this and other policies that are designed to achieve compliance with the Data Protection Legislation. (“the person responsible for data protection”).

No user within the authority shall deviate from this policy without written authorisation from the person responsible for data protection.

Erasure

Personal data should be erased when:

- The personal data is no longer necessary for the purpose which it was originally collected or processed. Normal retention periods are specified in the Privacy Notice.
- The authority is relying on consent as the lawful basis for processing the data, and the individual withdraws their consent.
- The authority is relying on legitimate interests as the basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing.

- The authority is processing the personal data for direct marketing purposes and the individual objects to that processing.
- The authority has processed the personal data unlawfully (i.e. in breach of the lawfulness requirement of the 1st principle).
- The authority has to do it to comply with a legal obligation.
- The authority has processed the personal data to offer information society services (that is online services) to a child.

The right to erasure does not apply if processing is necessary for one of the following reasons:

- To exercise the right of freedom of expression and information.
- To comply with a legal obligation.
- For the performance of a task carried out in the public interest or in the exercise of official authority.
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing.
- For the establishment, exercise or defense of legal claims.

The UK GDPR also specifies two circumstances where the right to erasure does not apply to special category data:

- If the processing is necessary for public health purposes in the public interest (eg protecting against serious cross border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices).
- If the processing is necessary for the purposes of preventative or occupational medicine; for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services. This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (e.g. a health professional).

Refusal

The Authority may refuse to comply with a request if it is:

- **Manifestly unfounded**
  A request may be manifestly unfounded if:
  - The individual clearly has no intention to exercise their right of

erasure. For example, an individual makes a request but then offers to withdraw it in return for some form of benefit from the authority.

- The request is malicious in intent and is being used to harass the authority with no real purposes other than to cause disruption.

- **Excessive**
  A request may be excessive if:

  - It repeats the substance of previous requests; or
  - It overlaps with other requests.
  - The person responsible for data protection shall decide if a request is manifestly unfounded or excessive on a case by case basis. The authority does not have a blanket policy on refusal.

All requests should be considered in the context in which it is made.

If a request is refused the person responsible for data protection should document why they consider the request is manifestly unfounded or excessive.

In the event of the right to erasure not being applicable or the authority refusing the request to erase, the person responsible for data protection will inform the individual without undue delay and within 1 month of receipt of the request and provide:

- The reasons the authority is not taking action.
- The individual's right to make a complaint to the ICO, and the individual's ability to seek to enforce this right through a judicial remedy.

Time limits

The person responsible for data protection must respond to an erasure request without undue delay and at the latest within 1 month with confirmation of erasure or reasons for refusal.

The time limit to respond starts on receipt of the request or (if later) on receipt of any information requested to confirm the requestor's identity.

The person responsible for data protection can extend the time to respond by a further two months if the request is complex or they have received a number of requests from the individual. The person responsible for data protection must let the individual know within 1 month of receiving their request and explain why the extension is necessary.

If the person responsible for data protection has doubts about the identity of the person making the request, they can ask for more information to identify them. They should only request information that is necessary to confirm identity. The person responsible for data protection must inform the individual without undue delay and within 1 month that they need more information to confirm identity.

Users Role in Erasure Requests

The authority has a legal responsibility to identify that an individual has made a request.

The UK GDPR does not specify how to make a valid request. A request can be made verbally or in writing. It can also be made to any part of the authority and does not have to be a specific person or contact point.

Users should be aware that requests can be made via email, or social media.

A request does not have to include the phrase 'request for erasure' or Article 17 of the UK GDPR.

Users must notify in writing the person responsible for data protection immediately and in any case within 1 working day of a request to erase.

No user should action the erasure request and erase data without first informing and getting authorisation from the person responsible for data protection.

Users must provide all timely assistance to the person responsible for data protection

Obstruction of a lawful erasure by a user will be addressed via the relevant disciplinary procedure.

Erasure of Data

When data is to be erased either because it is no longer required to fulfil the purpose for which it was collected or because there has been a valid request to erase from the data subject in question, the person responsible for data protection shall ensure that:

- Paper based personal data is crosscut shredded or disposed of via a secure disposal contractor who supplies a certificate of destruction, and / or

- Electronic records are removed from backup systems as well as live systems.

    - The Authority is aware that when data is deleted from the live system it will remain within the backup environment for a certain

period of time until it is overwritten.

- For erasure where the data is no longer required this time delay is acceptable and backups can be allowed to run to normal schedule as the data will be erased from them in due course.

- For data that has been requested to be erased the person responsible for data protection must confirm to the requester what will happen to their data when their erasure request is fulfilled, including in respect of backup systems, an indication should be given of how long it will take to purge from the backups.

- The person responsible for data protection should then ensure th at the data on the backup is 'beyond use' and that the data withi n the backup is not used for any other purpose.

- The person responsible for data protection must ensure that data that has been erased is not accidentally reintroduced in the event of a backup being re stored.

- When actioning erasure the person responsible for data protection shall ensure that the relevant data is erased from the entire filing system paying particular attention to file location whether centralised, decentralised or dispersed on a functional or geographical basis.

Updates to this Policy

This policy shall be reviewed annually by the person responsible for data protection.

This policy shall be reviewed if Penzance Town Council makes changes to the Authority Privacy Notice or if there are changes to how the authority processes data or the data protection legislation changes.

This policy was last updated on 16/3/2026.

Implementation

This policy takes effect from 16/3/2026 and is not retroactive.

PENZANCE COUNCIL

Data Retention & Disposal Policy

CURRENT POLICY STATUS

Version:	3	Approving Body:	Full Council
Date:	16/3/2026	Date of Approval:	16/03/2026
Responsible Officer:	Town Clerk	Minute Reference:	
Overview Committee:	Full Council	Review Date:	

VERSION HISTORY

DATE	VERSION	AUTHOR/EDITOR	COMMENTS
22/08/2023	2	SG	
16/3/2026			

REVIEW RECORD

DATE	TYPE OF REVIEW	COMPLETED BY
08/2023	Annual	CSM/Town Clerk/Council

~~1. INTRODUCTION~~

Formatted: Space After: 8 pt

~~Penzance Council recognises that the efficient management of its records is necessary to comply with legal and regulatory obligations and to ensure high standards of practice for the Council and its activities. This policy provides the framework through which this effective management can be achieved and recorded.~~

(V2) Approved and adopted by Penzance Council: 16 August 2023

Data Retention & Disposal Policy

~~1.1 The Council accumulates a vast amount of information and data during the course of its everyday activities. This includes data generated internally in addition to information obtained from individuals and external organisations. This information is recorded in various different types of document.~~

~~1.2 Records created and maintained by the Council are an important asset and as such measures need to be undertaken to safeguard this information. Properly managed records provide authentic and reliable evidence of the Council's transactions and are necessary to ensure it can demonstrate accountability.~~

~~1.3 Documents may be retained in either 'hard' paper form or in electronic forms. For the purpose of this policy, 'document' and 'record' refers to both hard copy and electronic records.~~

~~1.4 It is imperative that documents are retained for an adequate period of time. If documents are destroyed prematurely the Council and individual officers concerned could face prosecution for not complying with legislation and it could cause operational difficulties, reputational damage and difficulty in defending any claim brought against the Council.~~

~~1.5 In contrast to the above the Council should not retain documents longer than is necessary. Timely disposal should be undertaken to ensure compliance with the General Data Protection Regulations so that personal information is not retained longer than necessary. This will also ensure the most efficient use of limited storage space.~~

This policy sets out the procedures Penzance Town Council has in place for the retention and disposal of records held by the authority.

Penzance Town Council is a council in England.

Its contact details are:

Penzance Council,

Penlee Centre, Penlee Park, Penzance, TR18 4HE

The Council creates and receives a large volume of information in the course of its work. This includes records created internally and information received from individuals, businesses and other organisations.

Records may exist in paper form, electronic form or any other organised filing system.

Appropriate retention and timely disposal of records ensures that:

• the Council complies with legal and regulatory obligations

• information can be retrieved efficiently when required

• personal data is not retained longer than necessary

• storage systems remain manageable and secure

Failure to retain records for the correct period may expose the Council to legal risk. Conversely, retaining records longer than necessary may breach the storage limitation principle contained in the UK General Data Protection Regulation.TT

Data Protection Legislation

Formatted: Font: Bold

Penzance Town Council is a data controller for personal data as defined by applicable data protection and privacy legislation including:

• the retained EU law version of the General Data Protection Regulation (EU) 2016/679 (UK GDPR)
• the Data Protection Act 2018
• the Privacy and Electronic Communications Regulations 2003
• any successor legislation

Under Article 5(1)(e) of the UK GDPR personal data must be kept no longer than is necessary for the purposes for which it is processed.

This policy establishes the Council's retention schedule to ensure compliance with this requirement.

~~**2. RESPONSIBILITIES**~~

~~2.1 Penzance Council has a corporate responsibility to maintain its records and record management systems in accordance with current regulations and legislation. The Town Clerk has overall responsibility for the implementation of this policy and will provide guidance for good records management procedures and promote compliance with this policy so that information can be retrieved easily, appropriately and timely.~~

~~2.2 Individual employees must ensure that records for which they are responsible are accurate and are maintained and disposed of in accordance with the Council's records management guidelines. The retention schedule at Appendix 1 to this policy sets out the length of time records need to be kept and the action that should be taken when the documents are no longer required.~~

~~2.3 All employees are expected to manage their current record keeping systems in line with this retention schedule.~~

Person Responsible

The Town Clerk is responsible for the ongoing compliance monitoring of this and other policies that are designed to achieve compliance with the Data Protection Legislation. ("the person responsible for data protection").

The Town Clerk will:

- provide guidance on records management
- ensure that retention schedules are maintained
- ensure records are disposed of appropriately

Users

All officers, Members and volunteers handling Council information are responsible for ensuring that records under their control are:

- accurate
- stored securely
- retained only for the appropriate period
- disposed of in accordance with this policy

The retention schedule contained in Appendix A provides the minimum retention periods for common categories of Council records.

Suspension of Disposal

Where litigation, investigation, audit or freedom of information requests are anticipated or ongoing, records relevant to the matter must not be destroyed.

Disposal must be suspended until the matter has been fully resolved.

Aims

Formatted: No bullets or numbering

Formatted: Font: Bold

Formatted: Font: Bold

Formatted: Font: Bold

Data Retention & Disposal Policy

The aim of this document is to provide a working framework to determine which documents are:
• Retained – and for how long; or
Disposed of – and if so by what method

~~3. • DISPOSED OF~~ – AND IF SO BY WHAT METHOD~~SCOPE & OBJECTIVES OF THE POLICY~~

Formatted: No bullets or numbering

Formatted: Heading 1, Tab stops: Not at 1 cm

~~3.1 The aim of this document is to provide a working framework to determine which documents are:~~

- ~~Retained – and for how long; or~~
- ~~Disposed of – and if so by what method~~

~~3.2 There are some records that do not need to be kept at all or that are routinely destroyed in the course of business. This usually applies to information that is duplicated, unimportant or only of a short term value. Unimportant records of information include:~~

Formatted: Font: Bold

Principles

- ~~'With compliments' slips~~
- ~~Catalogues and trade journals~~
- ~~Non-acceptance of invitations~~
- ~~Trivial electronic mail messages that are not related to Council business~~
- ~~Requests for information such as maps, plans or advertising material~~
- ~~Out of date distribution lists~~

~~3.3 Duplicated and superseded material such as stationery, manuals, drafts, forms, address books and reference copies of annual reports may be destroyed.~~

Formatted: Indent: Left: 0 cm, First line: 0 cm

Formatted: Tab stops: Not at 1 cm

Some records do not require retention and may be destroyed in the normal course of business. This typically includes duplicated material, drafts, routine correspondence and documents of short-term administrative value. ~~3.4~~ Records should not be destroyed if the information can be used as evidence to prove that something has happened. ~~If destroyed the disposal needs to be disposed of under the General Data Protection Regulations~~

~~4. ROLES AND RESPONSIBILITIES FOR DOCUMENT RETENTION & DISPOSAL~~

Formatted: Indent: Left: 0 cm, Hanging: 0.76 cm, No bullets or numbering

~~4.1~~ Councils should have in place an adequate system for documenting the activities of their service. This system should take into account the legislative and regulatory environments ~~into~~ which they work.

Formatted: Indent: Left: 0 cm, First line: 0 cm

4.2 Records of each activity should be complete and accurate enough to allow employees and their successors to undertake appropriate actions in the context of their responsibilities to:

- Facilitate an audit or examination of the business by anyone so authorised.
- Protect the legal and other rights of the Council, its clients and any other persons affected by its actions.
- Verify individual consent to record, manage and record disposal of their personal data.
- Provide authenticity of the records so that the evidence derived from them is shown to be credible and authoritative
- To facilitate this, the following principles should be adopted:
  - Records created and maintained should be arranged in a record-keeping system that will enable quick and easy retrieval of information under the General Data Protection Regulations.
  - Documents that are no longer required for operational purposes but need retaining should be placed in the Penlee Centre's external archive store.

4.3 To facilitate this, the following principles should be adopted:

- Records created and maintained should be arranged in a record-keeping system that will enable quick and easy retrieval of information under the General Data Protection Regulations.
- Documents that are no longer required for operational purposes but need retaining should be placed in the Penlee Centre's external archive store.

4.4 The retention schedules in Appendix A: List of Documents for Retention or Disposal provide guidance on the recommended minimum retention periods for specific classes of documents and records. These schedules have been compiled from recommended best practice from the Public Records Office, the Records Management Society of Great Britain and in accordance with relevant legislation.

4.5 Whenever there is a possibility of litigation, the records and information that are likely to be affected should not be amended or disposed of until the threat of litigation has been removed.

5. DOCUMENT DISPOSAL PROTOCOL

5.1 Documents should only be disposed of if reviewed in accordance with the following:

Formatted

Formatted: Indent: Left: 0 cm, First line: 0 cm

Formatted: No bullets or numbering

- Is retention required to fulfil statutory or other regulatory requirements?
- Is retention required to meet the operational needs of the service?
- Is retention required to evidence events in the case of dispute?
- Is retention required because the document or record is of historic interest or intrinsic value?

~~5.2~~ When documents are scheduled for disposal the method of disposal should be ~~e~~ appropriate to the nature and sensitivity of the documents concerned. A record of the disposal will be kept to comply with the General Data Protection Regulations.

~~5.3~~ Documents can be disposed of by any of the following methods:

- Non-confidential records: place in ~~waste paper~~recycling bin for disposal.
- Confidential records or records giving personal information~~: shred documents~~ using crss shredding or secure confidential disposal. ~~.~~
- Deletion of computer records.
- Transmission of records to an external body such as the County Records Office at Kresen Kernow.

~~5.4~~ The following principles should be followed when disposing of records:

- All records containing personal or confidential information should be destroyed at the end of the retention period. ~~Failure to do so could lead to the Council being prosecuted under the General Data Protection Regulations.~~
- ~~the Freedom of Information Act or cause reputational damage.~~
- Where computer records are deleted steps should be taken to ensure that data is 'virtually impossible to retrieve' as advised by the Information Commissioner.
- Where documents are of historical interest it may be appropriate that they are transmitted to the County Records office.
- Back-up copies of documents should also be destroyed (including electronic or photographed documents unless specific provisions exist for their disposal).

5.5 Records should be maintained of appropriate disposals. These records should contain the following information:

- The ~~name~~ type of ~~the~~ document(s) destroyed.
- The date ~~the document was destroyed~~of destruction.
- The method of disposal.

~~6. DATA PROTECTION ACT 1998 – OBLIGATION TO DISPOSE OF CERTAIN DATA~~

Data Retention & Disposal Policy

~~The Data Protection Act 1998 controls how personal information is used by organisations, businesses or the government.~~

Under Article 5(1)(e) of the UK GDPR personal data must not be kept longer than is necessary for the purposes for which it is processed.~~6.1 The Data Protection Act 1998 ('Fifth Principle') requires that personal information must not be retained longer than is necessary for the purpose for which it was originally obtained. Section 1 of the Data Protection Act defines personal information as:~~

~~Data that relates to a living individual who can be identified:~~
~~a) from the data, or~~
~~b) from those data and other information which is in the possession of, or is likely to come into the possession of the data controller.~~

~~It includes any expression of opinion about the individual and any indication of the intentions of the Council or other person in respect of the individual.~~

~~6.2 The Data Protection Act provides an exemption for information about identifiable living individuals that is held for research, statistical or historical purposes to be held indefinitely provided that the specific requirements are met.~~

The authority ~~6.3 Councils are~~takes responsibility~~le~~ for ensuring that they comply with the principles of the General Data Protection Regulations, namely:

- Personal data is processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met.
- Personal data shall only be obtained for specific purposes and processed in a compatible manner.
- Personal data shall be adequate, relevant, but not excessive.
- Personal data shall be accurate and up to date.
- Personal data shall not be kept for longer than is necessary.
- Personal data shall be processed in accordance with the rights of the data subject.
- Personal data shall be kept secure.

~~6.4~~ External storage providers or archivists that are holding Council documents must also
comply with the above principles of the General Data Protection Regulations.

~~7. SCANNING OF DOCUMENTS~~

Formatted: No bullets or numbering

Scanned documents

Formatted: Font: Bold

Where paper records are scanned and stored electronically, the electronic version may be treated as the official record provided that it is a complete and accurate copy of the original.

Original documents may be securely destroyed once scanning and quality checks have been completed unless legislation requires the original to be retained.
Where required for audit, taxation or legal purposes, original documents must be retained for the period specified in the Council's retention schedule.

The Council will ensure that scanned records remain accessible, readable and securely stored for the duration of the applicable retention period.

7.1 In general once a document has been scanned on to a document image system the original becomes redundant. There is no specific legislation covering the format for which local government records are retained following electronic storage, except for those prescribed by HM Revenue and Customs.

7.2 As a general rule hard copies of scanned documents should be retained for three months after scanning.

7.3 Original documents required for VAT and tax purposes should be retained for six years unless a shorter period has been agreed with HM Revenue and Customs

8. REVIEW OF DOCUMENT RETENTION

8.1 It is planned to review, update and where appropriate amend this document on a regular basis (at least every three years in accordance with the *Code of Practice on the Management of Records* issued by the Lord Chancellor).

8.2 This document has been compiled from various sources of recommended best practice and with reference to the following documents and publications:

- *Local Council Administration*, Charles Arnold-Baker, 910h edition, Chapter 11
- Local Government Act 1972, sections 225 – 229, section 234
- SLCC Advice Note 316 Retaining Important Documents
- SLCC Clerks' Manual: Storing Books and Documents
- *Lord Chancellor's Code of Practice on the Management of Records* issued under Section 46 of the *Freedom of Information Act 2000*

9. LIST OF DOCUMENTS

9.1 The full list of the Council's documents and the procedures for retention or disposal can be found in Appendix A: List of Documents for Retention and Disposal. This is updated regularly in accordance with any changes to legal requirements.

Data Retention & Disposal Policy

Updates to this policy

This policy shall be reviewed annually by the person responsible for data protection.

This policy shall be reviewed if Penzance Town Council makes changes to the authority's Privacy Notice or if there are changes to how the authority processes data or the data protection legislation changes.

This policy was last updated on 16/3/2026

Implementation

This policy takes effect from 16/3/26 and is not retroactive.

~~**10. MONITORING AND REVIEW**~~

~~This policy will be monitored by the Town Clerk and reviewed regularly to ensure it is kept up to date and complies with current legislation.~~

Formatted: No bullets or numbering

Data Retention & Disposal Policy

APPENDIX 1

DATA RETENTION SCHEDULE

DOCUMENT	MINIMUM RETENTION PERIOD	REASON
Minutes & Correspondence		
Signed Council and Committee Minutes	Permanent archive	Legal requirement
Hand written notes from meetings	Destroy once typed up & approved at next meeting	To be available under the FOI Act
Agendas	Electronic copy – 5 years	Management
Correspondence & papers on important local issues & activities	5 years or until no longer valid / required	
Planning		
Planning applications lists + comments	On CC website; 4 years post decision	
Correspondence from residents	Until decision made by Committee	
Statutory documents, legislation, guidelines	Until no longer valid	
Finance		
Paid invoices	6 years	VAT
Cheque book stubs	Last completed audit year	
VAT records	6 years	VAT inspection
Supplier details/ Purchase orders	6 years	
Budgets & estimates	6 years	
Bank statements, incl. deposit & savings accounts	6 years	
Insurance policies	6 years from date on which insurance commenced/ was renewed	Statutory
Certificate of Employers Liability	40 years from date on which insurance commenced/was renewed	Employers' Liability (Compulsory Insurance) Regs. 1998 (SI 2753)
Insurance claims	6 years post settlement	
Pension records	6 years post employment	The Registered Pension Scheme (Provision of Information) Regulations 2006 (No. 18) – business data and documents

Formatted Table

		~~concerning pension schemes require a minimum storage time of 6 years.~~
~~Payroll documents (Inland Revenue)~~	~~6 years post employment~~	
~~Archive accounts/financial annual return~~	~~6 years~~	~~Audit, management~~
~~Financial Asset Register~~	~~10 years~~	~~Audit, management~~
~~Grant recipients~~	~~6 years~~	~~Audit, management~~
~~Leisure & Amenities~~		
~~Allotment Tenancy Agreements~~	~~Duration of tenancy + 2 years~~	~~Management~~
~~Allotment waiting list~~	~~Until allotment allocated or name withdrawn~~	~~Management~~
~~Car park quarterly permits~~	~~Until end of quarter~~	~~Management~~
~~Contractors – all related documents~~	~~Duration of contract + 1 year~~	~~Management~~
~~Unsuccessful tenders~~	~~6 months post campaign~~	~~Management~~
~~Play equipment inspection sheets~~	~~20 years~~	~~In case of claim~~
~~Penlee House~~		
~~Volunteers contact details~~	~~Duration of volunteering~~	~~Management~~
~~Friends of PH – contact details~~	~~4 years post membership~~	~~Management~~
~~Friends of PH – DD forms~~	~~6 years post membership~~	~~Management~~
~~Friends of PH – Gift Aid Declarations~~	~~6 years post membership~~	~~Management~~
~~Contractor documentation~~	~~Duration of contract + 1 year~~	~~Management~~
~~Public feedback forms~~	~~Digitised, anonymized & recorded; originals shredded within 1 year~~	~~Management~~
~~Loan forms~~	~~Duration of loan~~	~~Management~~
~~Donor records~~	~~Indefinite~~	~~Management~~
~~Orders (photography, shop)~~	~~Until completion of order~~	~~Management~~
~~Penzance Pass applications~~	~~Indefinite~~	~~Management~~
~~Photo permission forms~~	~~Indefinite~~	~~Management~~
~~Health & Safety~~		
~~H&S Accident Books~~	~~20 years~~	~~Legal requirement~~
~~Premises inspection records~~	~~20 years~~	~~In case of claim~~
~~Risk assessments~~	~~20 years~~	~~In case of claim~~
~~Equipment inspections~~	~~20 years~~	~~In case of claim~~
~~H&S Policy~~	~~Duration + 1 year~~	~~Management~~
~~HR Documents~~		
~~Timesheets~~	~~3 years~~	~~Management~~

~~Recruitment documents (incl. job announcements, job descriptions, person specifications)~~	~~6 years or until reviewed~~	~~Management~~
~~Job application documents (unsuccessful)~~	~~6 months~~	~~Data Protection~~
~~Personnel files & administration (not including payroll information), incl. CVs, annual appraisals, disciplinary records, sickness, annual leave, training records, contracts, redundancy, pay levels etc.~~	~~6 years post employment~~	~~Statutory (should a claim arise)~~
~~Statutory maternity/paternity pay & leave records~~	~~6 years post employment~~	~~Statutory~~

~~General Administration~~

~~Town Charter~~	~~Permanent archive~~	~~Historical document~~
~~Title Deeds, lease agreements~~	~~Indefinite~~	~~Audit, management~~
~~Members' Register of Interests~~	~~Duration of term as Councillor~~	~~Management~~
~~Newsletters, information etc. from other bodies~~	~~Until no longer relevant~~	
~~Corporate plans, strategies, policies, business plans, risk register, asset register~~	~~10 years~~	~~Audit, management~~
~~Complaints against the Council~~	~~6 years~~	~~Management~~
~~Complaints against Councillors~~	~~Term of office of Councillor~~	~~Management~~
~~Councillor contact details~~	~~Term of office~~	~~Management~~
~~Declarations of Interest~~	~~Term of office~~	~~Management~~
~~Community Group contact details~~	~~Until no longer relevant~~	~~Management~~
~~Civic invitee contact details~~	~~Until no longer relevant~~	~~Management~~
~~Routine correspondence, papers & emails~~	~~Unless relating to specific categories outlined in this document, kept for as long as needed for reference or accountability purposes~~	~~Regulatory, management, legal requirements~~
~~Local/historical information~~	~~Indefinite~~	

DATA RETENTION SCHEDULE

Council

DOCUMENT	MINIMUM RETENTION PERIOD	REASON
Signed Council and Committee Minutes	Permanent archive	Legal requirement
Agendas & Reports	Electronic copy – Permanent Archive	
Correspondence and Casework	1 year after conclusion of case	In case of return enquiries
Town CCTV	30 days	In case of requests to view
Office & Penlee House CCTV	28 days	In case of requests to view
Room bookings (free)	3 years	In case of liability claims
Room bookings (paid)	6 years	In case of liability claims

a. Planning

DOCUMENT	MINIMUM RETENTION PERIOD	REASON
Planning applications lists + comments	On CC website; in perpetuity in minutes as a matter of public record4 ~~years post decision~~	Public record
Correspondence from residents	Until decision made by Committee	
Statutory documents, legislation, guidelines	Until no longer valid	

b. Finance

DOCUMENT	MINIMUM RETENTION PERIOD	REASON
Paid invoices Cheque book stubs VAT records Supplier details/ Purchase orders Budgets & estimates	6 years	HMRC

Formatted Table

Data Retention & Disposal Policy

DOCUMENT	MINIMUM RETENTION PERIOD	REASON
Bank statements, incl. deposit & savings accounts		
Insurance policies	7 years after expiry	Statutory
Certificate of Employers Liability	7 years after expiry	Statutory
Insurance claims	7 years post decision	In case of further dispute
Pension records	6 years post employment	The Registered Pension Scheme (Provision of Information) Regulations 2006 (No. 18) - business data and documents concerning pension schemes require a minimum storage time of 6 years.
Payroll documents	6 years	HMRC
Archive accounts/financial annual return	6 years	Audit, management
Financial Asset Register Disposals	6 years	Audit, management
Grant & SLA recipients	Duration of project/contract plus 6 years	Audit, management
Tenancies	Duration of tenancy plus 2 years	In case of legal disputes after tenancy ends

Formatted Table

c. Leisure & Amenities

DOCUMENT	MINIMUM RETENTION PERIOD	REASON
Allotment Tenancy Agreements	Duration of tenancy + 2 years	GDPR & Data Protection In case of dispute after tenancy ends
Allotment waiting list	Until allotment allocated or individual withdraws their name	GDPR & Data Protection
Car park quarterly permits	Until end of quarter	GDPR & Data Protection
Contractors – all related documents	Duration of contract + 1 year	In case of liability claim or guarantee

DOCUMENT	MINIMUM RETENTION PERIOD	REASON
Contracts with extended liability including possible latent defects	12 years from completion of works or the expiry of the relevant obligation	Limitation Act 1980
Unsuccessful tenders including all related email correspondence and documents	6 months post campaign	GDPR & Data Protection
Play equipment inspection sheets	21 years	In case of claim
Memorials – family contact information	Permanent archive	
Use of Council land (free)	3 years	In case of claim
Use of Council land (paid)	6 years	In case of claim

Commented [BO1]: What about related email correspondence or related documents?

d. Penlee House

DOCUMENT	MINIMUM RETENTION PERIOD	REASON
Stewards and volunteers contact details	Whilst active volunteer (considered inactive after 6 months of no contact)	GDPR & Data Protection
Friends of PH – contact details	4 years post membership	GDPR & Data Protection
Contractor documentation	Duration of contract + 1 year	Management
Anonymous public feedback forms	Once digitised & recorded recycle	
Collections Management • Lenders • Borrowing institutions • Donors	Indefinitely	Historic record
Orders (photography, shop)	Until completion of order	
Penzance Pass records	2 years from issue	GDPR & Data Protection
Photo permission forms	Indefinite or until consent revoked by individual	GDPR & Data Protection
Photographs	Indefinitely or until consent revoked	Historic record
Website sales	3 months	GDPR & Data Protection
Enquiries & correspondence	Up to 7 years	
Community Engagement (including schools and education providers)	Until consent revoked by individual	GDPR & Data Protection

Formatted Table

DOCUMENT	MINIMUM RETENTION PERIOD	REASON
Invitations to gallery viewings	Until individual unsubscribes or revokes consent	GDPR & Data Protection

Formatted Table

e. Health & Safety

DOCUMENT	MINIMUM RETENTION PERIOD	REASON
H&S Accident Books	20 years	Legal requirement
Premises inspection records	20 years	In case of claim
Risk assessments	20 years	In case of claim
Equipment inspections	20 years	In case of claim
H&S Policy	Duration + 1 year	Management

f. HR Documents

DOCUMENT	MINIMUM RETENTION PERIOD	REASON
Recruitment documents (incl. job announcements, job descriptions, person specifications)	6 years or until reviewed	Management
Job application documents (unsuccessful)	6 months	Data Protection
Personnel files & administration (not including payroll information), incl. CVs, annual appraisals, disciplinary records, sickness, annual leave, training records, contracts, redundancy, pay levels etc.	6 years post employment	Statutory (should a claim arise)
Work experience documents (incl. applications, agreements, special category data)	Until end of placement	
Special category data collected for staff and Councillor training (consent needed) eg. Additional learning need	Duration of the training session only	
Statutory maternity/paternity pay & leave records	6 years post employment	Statutory
Councillor training records	Council term plus six years	

Formatted Table

Formatted: Not Highlight

Formatted: Not Highlight

g. Communications

DOCUMENT	MINIMUM RETENTION PERIOD	REASON
Council communications and community engagement • Invitations to meetings, civic events, and social events • Communicating changes to services • Consultations	Until 3 years of no response	
Subscribers to Council e-newsletter Subscribers to Penlee House e-newsletter	Until individual unsubscribes	

h. General Administration

DOCUMENT	MINIMUM RETENTION PERIOD	REASON
Town Charter	Permanent archive	Historical document
Title Deeds, lease agreements	Indefinite	Audit, management
Councillor Register of Interests	Duration of term as Councillor	Management
Newsletters, information etc. from other bodies	Until no longer relevant	
Corporate plans, strategies, policies, business plans, risk register, asset register	10 years	Audit, management
Complaints against the Council	6 years	Management
Complaints against Councillors	Term of office of Councillor	Management
Councillor contact details	1 council term after leaving	Management
Declarations of Interest	Term of officeviewing	Management
Community Group contact details	Until no longer relevant	Management

Data Retention & Disposal Policy

DOCUMENT	MINIMUM RETENTION PERIOD	REASON
Civic invitee contact details	3 years after last response or until consent withdrawn	Management
Routine correspondence, papers & emails	Unless relating to specific categories outlined in this document, kept for as long as needed for reference or accountability purposes	Regulatory, management, legal requirements
Local/historical information	Indefinite	
Room bookings (free)	3 years	In case of claim
Room bookings (paid)	6 years	In case of claim
Spiegelhalter Citizen Awards - nominations	Winner - indefinitely or until consent withdrawn Unsuccessful nominees – 12 months	
Spiegelhalter Citizen Awards - Awarding	Indefinitely or until consent withdrawn	
Photos – Council events, community events, cultural & historical records	Permanent archive	
Civic Chain record	3 years	In case of claim

PENZANCE COUNCIL

Subject Access Request Policy

CURRENT POLICY STATUS

Version:	1	Approving Body:	Council
Date:	16/3/2026	Date of Approval:	
Responsible Officer:	Town Clerk	Minute Reference:	
Overview Committee:	F&GP	Review Date:	16/3/2027

VERSION HISTORY

DATE	VERSION	AUTHOR/EDITOR	COMMENTS
16/3/2026	1	Cal Bagshaw CSM	New Policy

REVIEW RECORD

DATE	TYPE OF REVIEW	COMPLETED BY

This subject access request policy sets out the procedures Penzance Council has put in place to facilitate responding to subject access requests within the authority.

Penzance Town Council is a council in England.
Its contact details are:

Penzance Council,
Penlee Centre, Penlee Park, Penzance, TR18 4HE

Penzance Town Council is a data controller for personal data as defined by all applicable data protection and privacy laws including, but not limited to, the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (the "UK GDPR"), as it forms part of the law of England and Wales, Scotland, and Northern

Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 as amended, and any successor legislation (the “Data Protection Legislation”).

This policy is binding on all employees, members and volunteers (“User" or "Users”) of Penzance Town Council (“The Organisation”) in order to protect Personal or other Data ("Personal Data" or "Data”) processed by the organisation.

It applies to all organised filing systems be they computer based, paper based or any other such method of organising information which is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis (“Filing Systems”).

Definition of personal data

“Personal data” means any information relating to an identified or identifiable individual (“data subject”); an identifiable individual is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

Personal data will typically contain information about the individual or their activities.

Who is responsible for managing subject access requests

The Town Clerk is responsible for the ongoing compliance monitoring of this and other policies that are designed to achieve compliance with the Data Protection Legislation (“the person responsible for data protection”).

No user within the organisation shall deviate from this policy without written authorisation from the person responsible for data protection.

Subject access request

Individuals have the right to access and receive a copy of their personal data, and other supplementary information.

Subject Access Request (“SAR”) is a legal mechanism that has a very strictly defined and specific ambit.

It is a right that entitles a data subject to be informed by the organisation as to whether and how the organisation processes their personal data, a copy of that data and other supplementary information.

The parameters of the right are set out clearly in the UK GDPR which provides that a data subject “shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data”.

Subject access request is not a right to request ‘documents’ and is different to the freedom of information laws.

The authority believes that the right of access is key to allowing individuals to have real control over their own personal data. However, there are times when the right of access can be refused wholly or partially.

A subject access request can be refused if it is:

- Manifestly unfounded. A request may be manifestly unfounded if:
    - The individual clearly has no intention to exercise their right of access. For example an individual makes a request, but then offers to withdraw it in return for some form of benefit from the organisation, or
    - The request is malicious in intent and is being used to harass the organisation with no real purposes other than to cause disruption.

- Excessive. A request may be excessive if:
    - It repeats the substance of previous requests; or
    - It overlaps with other requests.

The person responsible for data protection shall decide if a request is manifestly unfounded or excessive on a case-by-case basis. The authority does not have a blanket policy on refusal.

All requests should be considered in the context in which they are made.

If a request is refused the person responsible for data protection should document why they consider the request is manifestly unfounded or excessive.

In the event of refusal of a subject access request the person responsible for data protection will inform the individual without undue delay and within 1 month of receipt of the request and provide:

- The reasons the authority is not taking action;
- Their right to make a complaint to the ICO and,
- Their ability to seek to enforce this right through a judicial remedy.

There are other exemptions that the person responsible for data protection must consider when preparing to disclose personal data to a SAR requestor.

If the response to the request would disclose personal data of another individual the person responsible for data protection shall make sure that the information has been redacted with a suitable redaction tool or method to maintain the confidentiality of the third party individual(s).

Schedules 2 and 3 of the UK Data Protection Act 2018 provide various other exemptions from subject access requests, the person responsible for data protection shall take professional advice on correct application of these exemptions if they are to be relied upon:-

- Crime and taxation: general.
- Crime and taxation: risk assessment.
- Legal professional privilege.
- Functions designed to protect the public.
- Regulatory functions relating to legal services, the health service and children's services.
- Other regulatory functions.
- Judicial appointments, independence and proceedings.
- Journalism, academia, art and literature.
- Research and statistics.
- Archiving in the public interest.
- Health, education and social work data.
- Child abuse data.
- Management information.
- Negotiations with the requester.
- Confidential references.
- Exam scripts and exam marks.
- Other Exemptions

Time limits

The person responsible for data protection must respond to a subject access request without undue delay and at the latest within 1 month with a copy of the personal data and other supplementary information or reasons for whole or partial refusal.

The time limit to respond starts on receipt of the request or (if later) on receipt of any information requested to confirm the requestor's identity.

The person responsible for data protection can extend the time to respond by a further two months if the request is complex or they have received a number of requests from the individual. The person responsible for data protection must let the individual know within 1 month of receiving their request and explain why the extension is necessary.

If the person responsible for data protection has doubts about the identity of the person making the request they can ask for more information to identify them. They should only request information that is necessary to confirm identity. The person responsible for data protection must inform the individual without undue delay and within 1 month that they need more information to confirm identity.

Users role in subject access requests

The authority has a legal responsibility to identify that an individual has made a request.

The UK GDPR does not specify how to make a valid request. A request can be made verbally or in writing. It can also be made to any part of the organisation and does not have to be to a specific person or contact point.

Users should be aware that requests can be made via email or social media.

A request does not have to include the phrases 'subject access request', ‘right of access’ or ‘Article 15 of the UK GDPR’.

Users must notify in writing the person responsible for data protection immediately and in any case within 1 working day of a subject access request or suspected subject access request.

No user should action the subject access request and gather personal data without first informing and getting authorisation from the person responsible for data protection.

Users must provide all timely assistance to the person responsible for data protection in their gathering and preparation of personal data for a subject access request.

Obstruction of the collection of personal data for a subject access request by a user will be addressed via the relevant disciplinary procedure.

Supply of personal data to the requestor

The right of access also entitles an individual to other supplementary information.

- The authority’s purposes for processing;
- Categories of personal data the authority is processing;
- Recipients or categories of recipient the authority has or will be disclosing the personal data to (including recipients or categories of recipients in third countries or international organisations);
- The authority’s retention period for storing the personal data or, where this is not possible, the criteria for determining how long the organisation will store it;
- The individual’s right to request rectification, erasure or restriction or to object to processing;
- The individual’s right to lodge a complaint with the Information Commissioner’s Office (ICO);
- Information about the source of the data, if the authority did not obtain it directly from the individual;
- Whether or not the authority uses automated decision-making (including profiling) and information about the logic involved, as well as the significance and envisaged consequences of the processing for the individual; and
- The safeguards the authority has provided where personal data has or will be transferred to a third country or international organisation.

The person responsible for data protection should ensure that all of the above items of supplementary information are detailed in the authority's privacy notice.

- If they are not, the privacy notice should be updated without delay, or

- If they are, the requirement to supply supplementary information can be complied with by supplying a copy of the organisations privacy notice.

If the individual submitted the SAR electronically (e.g. by email or via social media), The person responsible for data protection must provide the supplementary information and a copy of the personal data in a commonly used electronic format.

The person responsible for data protection may choose the format, unless the requester makes a reasonable request for it to be provided in another commonly used format (electronic or otherwise).

If the individual submitted the SAR by other means (e.g. by letter or verbally), the person responsible for data protection can provide a copy in any commonly used format (electronic or otherwise), unless the requester makes a reasonable request for it to be provided in another commonly used format.

The person responsible for data protection should ensure that the transfer of the personal data to the requester is done via an appropriately secure method.

The right of access enables individuals to obtain their personal data rather than giving them a right to see copies of documents containing their personal data.

The person responsible for data protection may therefore provide the information in the form of transcripts of relevant documents (or of sections of documents that contain the personal data), or by providing a print-out or copy of the relevant information from the authority's filing system.

When supplying in a commonly used format the requester must not be required to take any specific action in order to access the data. For example, being required to buy or download software.

If the requester asks for the information in hard copy, Royal Mail special delivery is considered a secure method of sending the information.

The person responsible for data protection may need to explain some of the information provided when responding to a SAR if the individual may have difficulty understanding it.

Updates to this policy

This policy shall be reviewed annually by the person responsible for data protection.

This policy shall be reviewed if Penzance Town Council makes changes to the authority’s Privacy Notice or if there are changes to how the authority processes data or the data protection legislation changes.

This policy was last updated on 16/3/26.

Implementation
This policy takes effect from 16/3/26 and is not retroactive.

Privacy Notice

Penzance Town Council

This privacy notice is intended to inform you of how your personal data will be used by the authority. The Council takes your data protection rights seriously and will only use your personal data in the ways described here.

Who we are and what we do?

Penzance Town Council is a council in England.

Its contact details are
Penzance Council, Penlee Centre, Penlee Park, Penzance, TR18 4HE.

The Council is a data controller for personal data as defined by all applicable data protection and privacy laws including, but not limited to, the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (the "UK GDPR"), as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 as amended, and any successor legislation (the "Data Protection Legislation").

The Council is not required to have a Data Protection Officer as defined by Article 37 of the UK GDPR.

The Council processes your personal data to enable it to manage the authority and provide a service to you and others.

Your data protection rights

Under the data protection legislation, you have rights including:

- Your right to be informed - You have the right to be informed of the Council's use of your personal data. This notice is designed to give you that information. If you require further information please make contact using the details below.
- Your right of access - You have the right to ask the Council for copies of your personal information.
- Your right to rectification - You have the right to ask the Council to rectify information you think is inaccurate. You also have the right to ask the Council to complete information you think is incomplete.

- Your right to erasure - You have the right to ask the Council to erase your personal information in certain circumstances.
- Your right to restriction of processing - You have the right to ask the Council to restrict the processing of your information in certain circumstances.
- Your right to object to processing - You have the right to object to the processing of your personal data in certain circumstances.
- Your right to data portability - You have the right to ask that the Council transfers the information you gave it to another organisation, or to you, in certain circumstances.
- Your right in relation to automated decision making including profiling – the Council does not process personal data in this way.

You are not required to pay any charge for exercising your rights. If you make a request, the law gives the Council one month to respond to you but it has undertaken to respond as soon as possible and in any case 1 month.

Please contact us using the details in Section 1 above if you wish to make a request.

What data does the data protection legislation cover?

Data protection legislation is to protect the data privacy of individuals and uphold your rights over your own personal data.

Definitions:

- Personal Data - means any information relating to an identified or identifiable person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.
- Processing - means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- Data Controller - means the person or organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- Data Processor - means a person or organisation which processes personal data on behalf of the Data Controller.
- Third Country - means a country or territory outside the United Kingdom.
- Lawful Basis - means one of the six lawful reasons to process personal data as set out in Article 6 of the UK GDPR. At least one of these will apply whenever we process your personal data.

Why does the Council have your information and how long will it keep it?

- The Council takes your data privacy seriously and will only use your personal data for the purpose for which it was collected.
- For every activity that the Council undertakes using personal data it must be clear what its purpose is for that activity and have a Lawful Basis to process your data.
- Where the Council processes personal data that reveals special category data (article 9 UK GDPR) or personal data relating to criminal convictions and offences (article 10 UK GDPR) it requires an additional condition to process.
- The Council collects and processes your personal data for the following purposes for which it collects certain categories of data and in order to lawfully process your data for those purposes it relies on these lawful bases and additional conditions.

Purpose	**Lawful basis**	**Additional Condition to Process**	**Categories of data**
Minutes	Legal obligation	N/A	Identity Contact
Accounts	Legal obligation	N/A	Identity Contact Special category data Other Council Contractors Job title
Correspondence and Casework	Public Task	Article 9(g) substantial public interest	Identity Contact Bank Details Pension details Special category data Job title
Payroll	Legal obligation	Article 9(b) employment and social security and social protection	Identity Contact Bank Details

Planning	Public Task	N/A	Identity Contact
Tenancies	Contract	Article 9(g) substantial public interest	Identity Contact Special category data Salary details
HR	Contract	Article 9(b) employment and social security and social protection	Identity Contact
Training	Contract	Article 9(b) employment and social security and social protection	Identity Contact
Training	Public Task	Article 9(a) explicit consent	Identity Contact Special category data Qualifications Employment history
Recruitment	Contract	Article 9(b) employment and social security and social protection	Identity Contact Image Special category data
Town CCTV	Legitimate Interest	Article 9(e) manifestly made public	Image
Office CCTV	Legitimate Interest	Article 9(g) substantial public interest	Image

Room Bookings (free)	Legitimate Interest	N/A	Identity Contact
Room Bookings	Contract	N/A	Identity Contact Special category data
Communications and community engagement	Legitimate Interest	Article 9(a) explicit consent	Identity Contact Special category data
Communications and community engagement (Email)	Consent	Article 9(a) explicit consent	Identity Contact
Use of Council Land (free)	Legitimate Interest	N/A	Identity Contact
Use of Council Land	Contract	N/A	Identity Contact
Website sales	Contract	N/A	Identity Contact
Penzance Pass Records	Consent	N/A	Identity Contact
Invitations to Gallery viewings	Legitimate Interest	N/A	Identity Contact
Collections Management	Legitimate Interest	N/A	Identity Contact

Penlee House stewards and volunteers	Legitimate Interest	Article 9(a) explicit consent	Identity Contact
Penlee House Enquiries and Correspondence	Legitimate Interest	Article 9(a) explicit consent	Identity Contact Special category data
Penlee House Community Engagement	Legitimate Interest	Article 9(a) explicit consent	Identity Contact Special category data
Penlee House Community Communications	Consent	Article 9(a) explicit consent	Identity Contact
Friends of Penlee House Membership	Contract	N/A	Identity Contact Special category data
Allotments	Contract	Article 9(a) explicit consent	Identity Contact Vehicle details
Car Parking Permits	Contract	N/A	Identity Contact
Memorials	Contract	N/A	Identity Contact
Strategic partnerships	Contract	N/A	Identity Contact Special category data
Awards Nominations	Legitimate Interest	N/A	Identity Contact

Awards Awarding	Consent	Article 9(a) explicit consent	Identity Contact
Photographs	Legitimate Interest	Article 9(e) manifestly made public	Image
Photographs	Consent	Article 9(a) explicit consent	Image
Register of Interest	Legal obligation	Article 9(g) substantial public interest	Identity Contact
Councillor Information	Public Task	Article 9(g) substantial public interest	Identity Contact Special Category Data

If the Council has relied on 'consent' to process your personal data, you are able to withdraw that consent at any time and it will assist you.

The Council collects data in the following ways

Categories of data	**How we collect your data**
Bank Details	Direct from you
Contact	Direct from you Cornwall council
Employment history	Direct from you
Identity	Direct from you Cornwall council
Job title	Direct from you
Other Council Contractors	Direct from you
Pension details	Direct from you
Qualifications	Direct from you
Salary details	Direct from you
Special category data	Direct from you From Someone who has nominated you for

Vehicle details	Direct from you

How long the Council intends to keep your data

Purpose	**How long we will keep your data**
Minutes	Permanent Archive
Accounts	6 years
Correspondence and Casework	1 year after conclusion of case
Payroll	6 years
Planning	Permanent archive
Tenancies	Duration of tenancy plus 2 years
HR	6 years post employment
Training	6 years post employment
Recruitment	6 months
Town CCTV	30 days
Office CCTV	28 days
Room Bookings (free)	3 Years After Booking
Room Bookings	6 Years After Booking
Communications and community engagement	Until 3 years of no response
Communications and community engagement (Email)	Until unsubscribe

Use of Council Land (free)	3 Years after booking
Use of Council Land	6 Years after booking
Website sales	3 months
Penzance Pass Records	2 years from issue
Invitations to Gallery viewings	Until unsubscribe
Collections Management	Indefinitely
Penlee House stewards and volunteers	Whilst active volunteer
Penlee House Enquiries and Correspondence	Up to 7 years
Penlee House Community Engagement	Until consent revoked
Penlee House Community Communications	Until unsubscribe or unconsent
Friends of Penlee House Membership	4 years post membership
Allotments	Duration of tenancy + 2 years
Car Parking Permits	Until end of the quarter
Memorials	Permanent Archive
Strategic partnerships	6 Years after contract
Awards Nominations	12 months

Awards Awarding	Until consent withdraw
Photographs	Permanent archive
Photographs	Permanent archive
Register of Interest	Until they are no longer a councillor and have been replaced by a new councillor.
Councillor Information	1 council term after leaving

When the Council no longer needs your personal data to undertake its stated purpose it will delete it or anonymise it so that it no longer permits the identification of you.

Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with UK GDPR Article 89(1).

In some cases the Council may be allowed to use your personal data to contact you with news about its activities, products or services. The Council will always offer an opt out and will always comply with the data protection legislation.

Sharing this information with other data controllers

The Council may share your data with another data controller if that controller takes over the purpose for which it collected your data.

The Council may be required to share your personal data for legal, judicial, law enforcement or government reasons.

We routinely share personal data with other data controllers for the following reasons.

Purpose	**Receiving Data Controller**	**Data Controller Location**
Accounts	HMRC	UK EU
Correspondence and Casework	Other Local Authority Expert Helpers Law enforcement and similar competent authorities Contractors and suppliers Members of the public Officers	UK EU

Payroll	HMRC Pension Provider	UK EU
Planning	Other local authority	UK
HR	Other local authority	UK
Training	Other local authority Council associations Worknest iHasco First Aid Cornwall High Speed Training ROSPA Liam Cottrell Kernow Lantra Training HSQE Breakthrough Communications Fire Safety Cornwall Cornwall College Corserv	UK EU
Training	Other local authority Council associations NALC SLCC Worknest iHasco Breakthrough Communications	UK EU
Town CCTV	Law enforcement and similar competent authorities	UK
Office CCTV	law enforcement and similar competent authorities	UK
Photographs	Press and media Social media	UK EU

Register of Interest	Other local authority	UK
Councillor Information	Other local authority	UK

The Council may share your personal data with other data controllers to enable it to fulfil its obligations to you or to provide a product or service, in that event it will tell you who it is going to share your data with.

The Council takes your data protection rights seriously and will take steps to ensure that those it shares data with process it responsibly.

Data processors working on the Council's behalf

The Council may send your data to a data processor to undertake data processing activities on its behalf.

The Council sends personal data to data processors for the following reasons.

Categories of data processor	**Purpose**	**Data Processor Location**
AdvantEdge	Accounts Room Bookings Use of Council Land Friends of Penlee House Membership Allotments Car Parking Permits Memorials Strategic partnerships	EU
Canva	Communications and community engagement Communications and community engagement (Email) Photographs Photographs Councillor Information	Australia
Collections database - Modes Complete	Collections Management Friends of Penlee House Membership Strategic partnerships	UK
Health Assured	Employee Assistance Provider	UK
Mailchimp	Communications and community engagement Communications and community engagement (Email)	USA

	Website sales Invitations to Gallery viewings Penlee House Community Engagement Penlee House Community Communications Strategic partnerships Photographs	
Microsoft	Minutes Accounts Correspondence and Casework Payroll Planning Tenancies HR Training Training Recruitment Office CCTV Room Bookings (free) Room Bookings Communications and community engagement Communications and community engagement (Email) Use of Council Land (free) Use of Council Land Website sales Penzance Pass Records Invitations to Gallery viewings Collections Management Penlee House stewards and volunteers Penlee House Enquiries and Correspondance Penlee House Community Engagement Penlee House Community Communications Friends of Penlee House Membership Allotments Car Parking Permits Memorials Strategic partnerships Awards Nominations Awards Awarding Photographs Photographs Register of Interest Councillor Information	UK

Online payment link provider	Allotments Car Parking Permits	UK
Payroll provider	Payroll	EU
Royal Mail	Website sales	UK
Security contractor	Town CCTV	UK
SumUp payment provider	Accounts Allotments Car Parking permits	EU
Website server provider	Minutes Planning Communications and community engagement Communications and community engagement (Email) Website sales Penlee House Enquiries and Correspondence Penlee House Community Engagement Penlee House Community Communications Friends of Penlee House Membership Car Parking Permits Strategic partnerships Awards Awarding Photographs Photographs Register of Interest Councillor Information	UK
Worknest	HR	UK
Worksmarter	HR	UK

Where does the Council store and process your personal data?

Most of your personal data will be stored and processed here in the UK.

Some data may be stored or processed in other third countries. The Council has made sure that safeguards are in place on such transfers to ensure that an equivalent standard of data protection is in place.

Personal data transferred to EU member states, Iceland, Norway, Liechtenstein, Gibraltar, Andorra, Argentina, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland, Uruguay, Japan (only private sector organisations) or Canada (only covers data that is subject to Canada's Personal Information Protection and Electronic Documents Act) is transferred to those third countries on the basis of adequacy regulations.

Personal data transferred to USA organisations certified to the "UK Extension to the EU-US Data Privacy Framework" is transferred on the basis allowed for by Article 45 of the UK General Data Protection Regulation (GDPR).

Personal data transferred to other USA organisations and all other countries is transferred on the basis of International Data Transfer Agreements (IDTAs) where there is a contract incorporating an agreement recognised or issued in accordance with the data protection legislation. The IDTA contains contractual obligations on us (the data exporter) and the receiver (the data importer), and rights for the individuals whose personal data is transferred.

How to contact the Council for more information

If you have any questions, wish to exercise any of your data protection rights or have a complaint please contact Penzance Town Council, Penlee Centre, Penlee Park, Penzance, TR18 4HE.

You can also complain to the Information Commissioner's Office (ICO) if you are unhappy with how the Council has used your data. Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF Helpline number: 0303 123 1113

Updates to this notice

The Council might have to make changes to this Privacy Notice if there are changes to how it processes your personal data or the data protection legislation changes.

Changes will be made available via updated notices on the Penzance Town Council Website and at the Penzance Town Council offices at the above address.

This Privacy Notice was last updated on 16/3/26.

PENZANCE COUNCIL – 16 MARCH 2026

REPORT FOR DECISION

VIREMENT OF FUNDS FOR ONGOING PROJECTS

Our Culture	Our Decision Making	Our Environment	Our Money	Our People	Our Places	Our Resilience & Wellbeing
	✓		✓			

Recommendation:

1. The remaining balance of the Wellfields Car Park – Capital Works budget (1060/7), as of 31 March 2026, be transferred to the Wellfields Car Park earmarked reserve and expenditure from said reserve be authorised up to said amount in order to progress the project(s) detailed in this report.

2. The remaining balance of the Coach House – Capital Refurbishment budget (4100/7/5), as of 31 March 2026, be transferred to the Coach House Refurbishment earmarked reserve.

Background:

Due to capital projects spanning over two financial years, by default any remaining budget would be transferred to the General Fund balance in the new financial year. It is therefore necessary to transfer funds prior to the new year to the respective earmarked reserves to then draw down when required.

Leisure and Amenities – Wellfields Car Park Capital Works

The budget allocated to Wellfields Car Park Capital Works for £20,000 was agreed to carry out preliminary works for the car park re-design to improve the layout, safety of pedestrian access and upgrades to drainage. An initial piece of work was contracted during the year for different designs of a new car park layout, but there are still works needed before a final proposal can be taken back to committee before carrying out the project. It is therefore recommended that the remaining budget (currently £18,300) is transferred to the Wellfields Car Park reserve before the new financial year to earmark this funding and allow it to be drawn down when required.

Arts and Culture – The Coach House Capital Refurbishment

The Coach House Café refurbishment project is coming to an end; it is recommended that any remaining balance left in the budget at the end of the financial year is transferred back into the Coach House Refurbishment Reserve for any future costs to draw down when required as these funds are specifically budgeted for this project and not general expenditure.

Cameron Sil
Finance Manager

PENZANCE COUNCIL – 16 MARCH 2026

REPORT FOR DECISION

PROVISION OF VEHICLE ACTIVATED SPEED WARNING SIGNS

Our Culture	Our Decision Making	Our Environment	Our Money	Our People	Our Places	Our Resilience & Wellbeing
		✓	✓	✓	✓	

Recommendation:

1. The use of up to £7,000 from the Climate Emergency Initiatives budget (2200/3) be approved for the purchase of two Vehicle Activated Speed Warning Units, as detailed in Appendix 2 to this report, and any associated equipment for their operation.

2. Authority be delegated to the Town Clerk to determine the locations of the units throughout the parish, and their length of time therein, in accordance with those detailed within Appendix 1 to this report.

3. Should it be necessary, representations be made to the Highways Authority and/or Devon and Cornwall Police, following consultation with the appropriate ward Councillors, as a result of the data provided by said units.

4. A report be provided to a future meeting of the Council to detail the experience of using said units following twelve months of their operation.

Background:

Penzance Council resolved to procure a Vehicle Activated Speed Warning Sign for use on a rotational basis within problem speeding areas within the Penzance Parish. Authority was delegated to the Town Clerk to develop a policy to identify locations for installation, based on need, existing mounting locations, CC Highways approvals and to consider further issues that may arise as part of a deployment.

Following initial discussions, there was a need to tie in with Cornwall Council's roll out of the '20 is Plenty' initiative and the Town Deal Sustainable Transport programme.

Both of which are delivering significant highways infrastructure changes as well as considerable additional signage, new crossings and the introduction of a funded vehicle activated sign on New Rd.

Now that both programmes are in their final stages of delivery the Town Clerk collated historic location requests and undertook Parish wide site visits with the Highways Area Manager. The site visits considered historically raised issues but importantly identified existing Highways assets which would meet practical and safety requirements for installation of signs. Following the audit and inspections, Appendix 1 details eleven exact locations where approval is now in place for the installation of Vehicle Activated Speed Warning Signs (VAS).

Appendix 2 details the specification of Vehicle Activated Sign that is proposed. Classed as mobile, they can easily be mounted and dismounted and relocated to the different proposed sites around the Parish. Wired connection is not possible and due to the restrictive locations and potential wind stress, the solar panel option has to be ruled out.

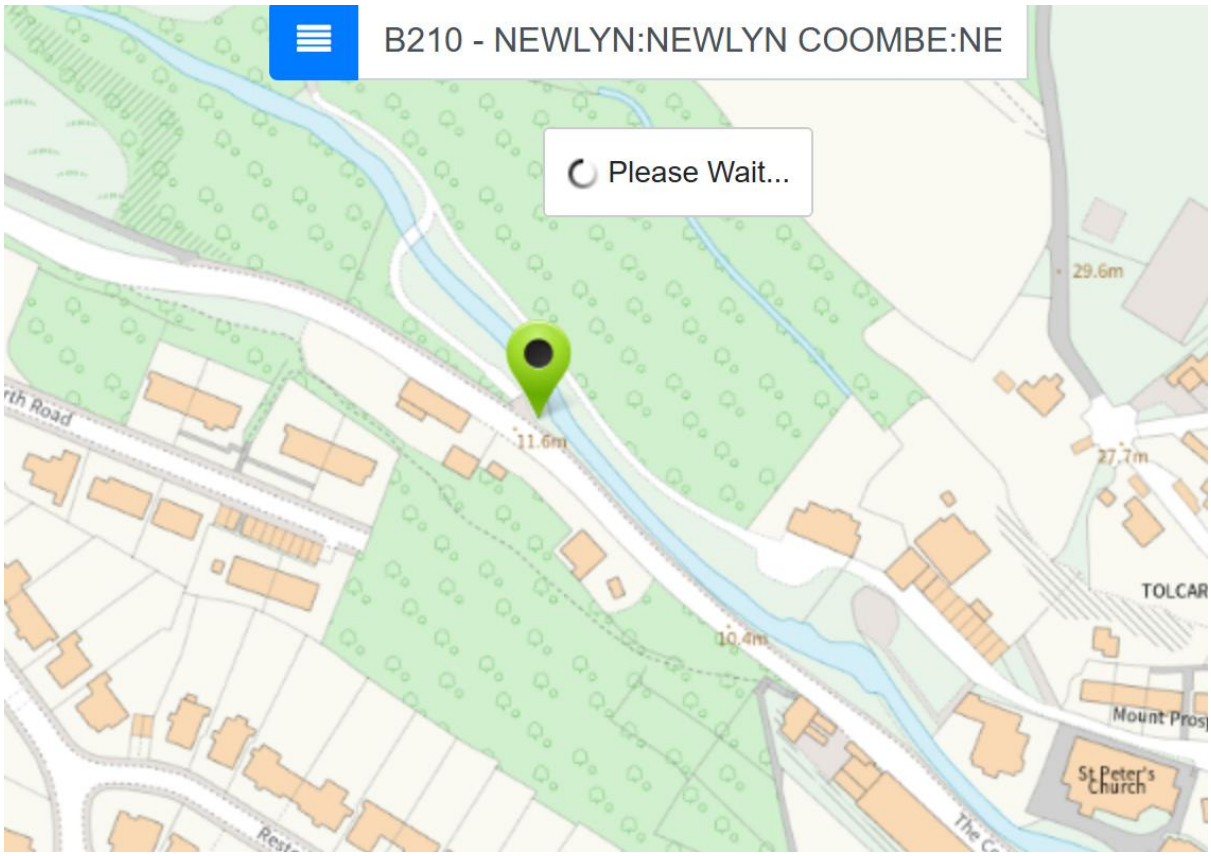
Potential officer time costs for ongoing operations is hard to gauge. The battery-operated units once situated will require a battery change every 1-2 weeks along with data collection from the units which can be done via Bluetooth when changing the batteries. Information from suppliers and testimonials suggest battery changes take half hour per change-over. Relocating between sites can be done by one officer and would take an hour or two every few months/depending on frequency of movement.

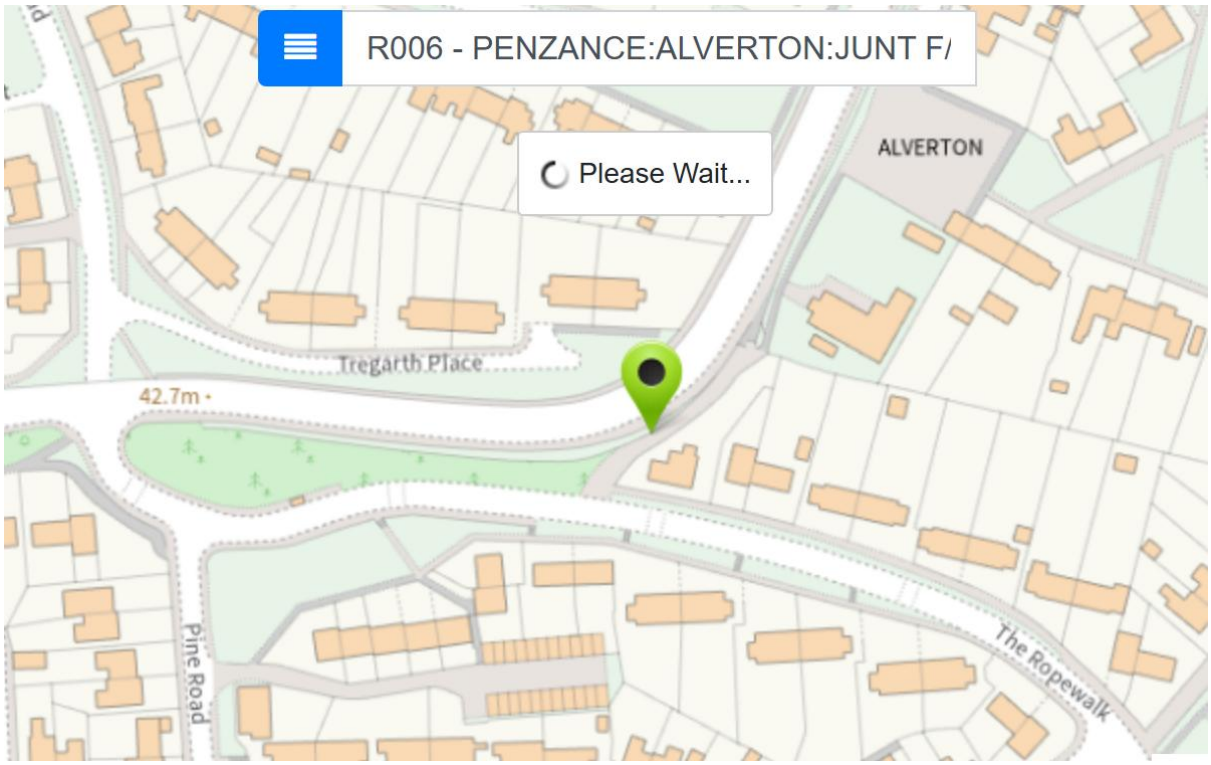
Excess speed is still often identified as a risk across the Parish, this initiative will contribute to community safety, lower speeds helps to reduce emissions and enable us to respond to issues raised in specific locations. Council support is sought for up to £7,000 of expenditure from Budget 2200/3 Climate Emergency initiatives for the purchase of 2 VAS units which will be rotated around the identified locations on a 3 monthly basis, prioritised through discussion and monitoring with the Highways Manager.

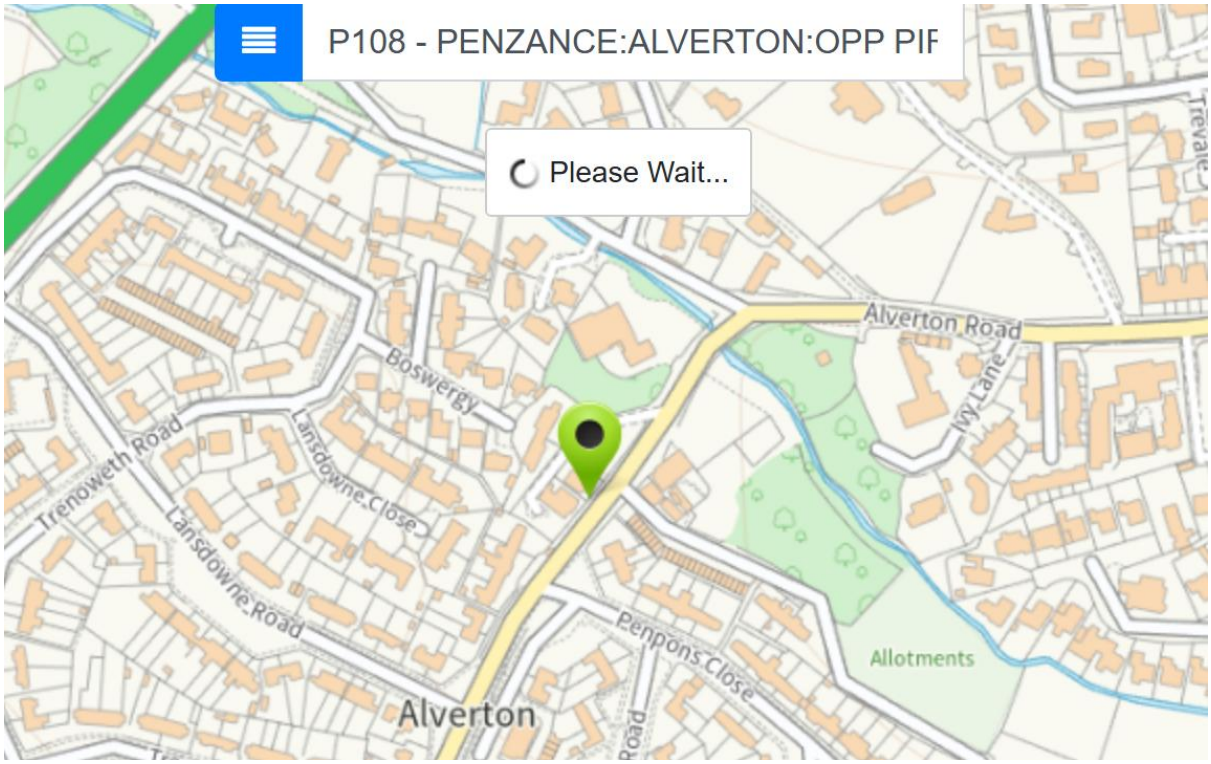
Appendix 1 – Initial Locations for Speed Warning Signs
Appendix 2 – Proposed Vehicle Activated Speed Warning Signs Specification

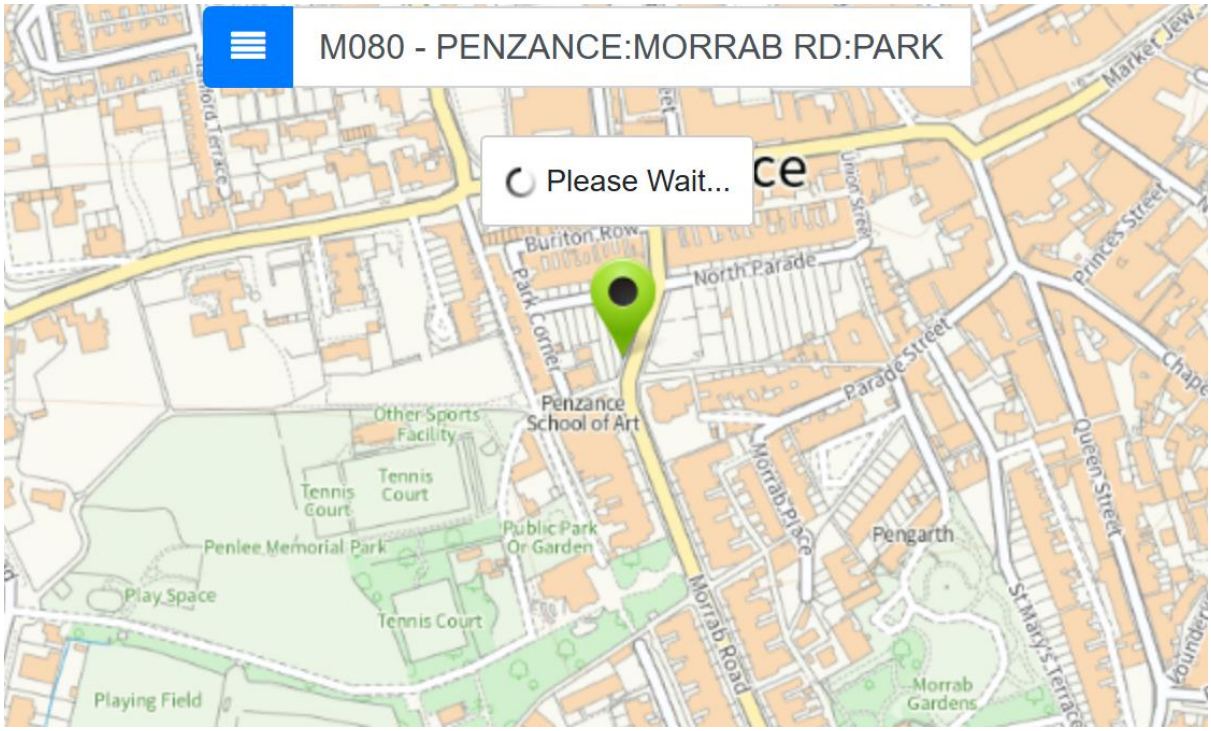
James Hardy
Town Clerk

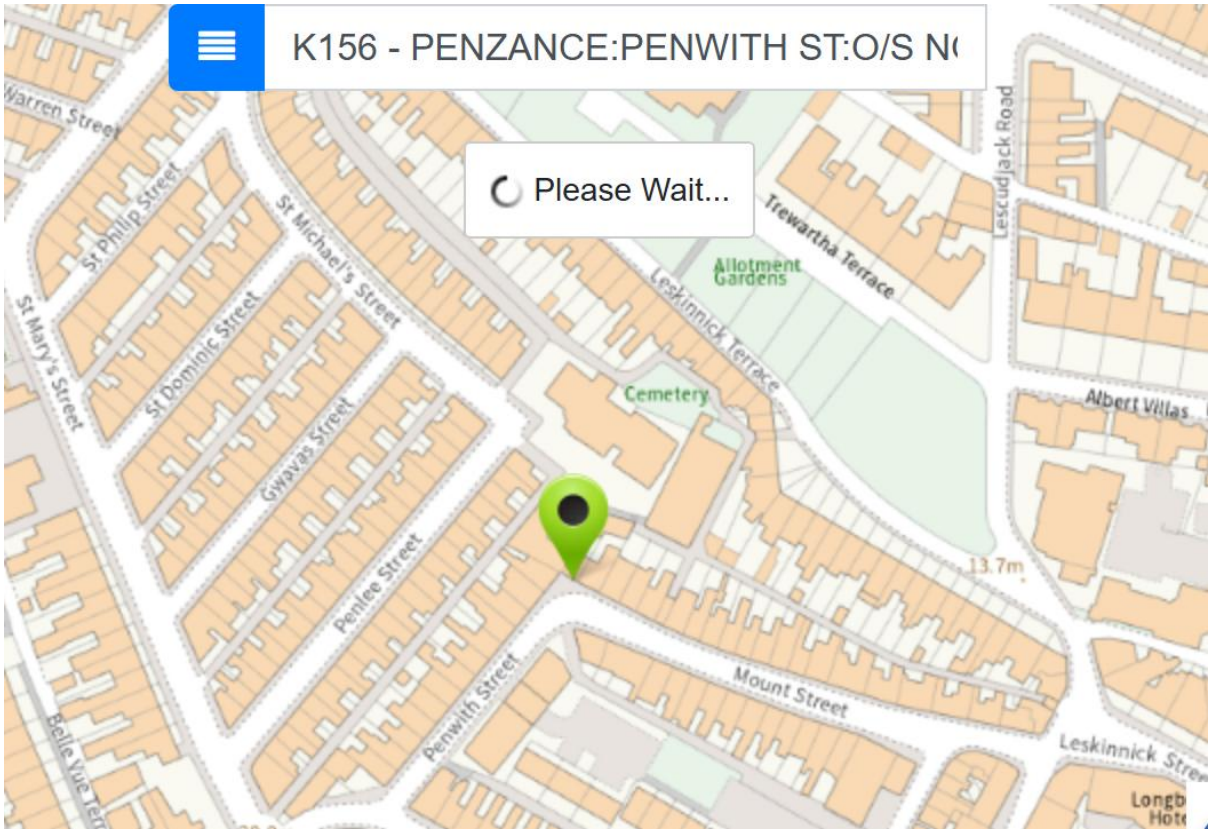
Penzance Council – CC Highways approved Vehicle Activated Sign installation locations.





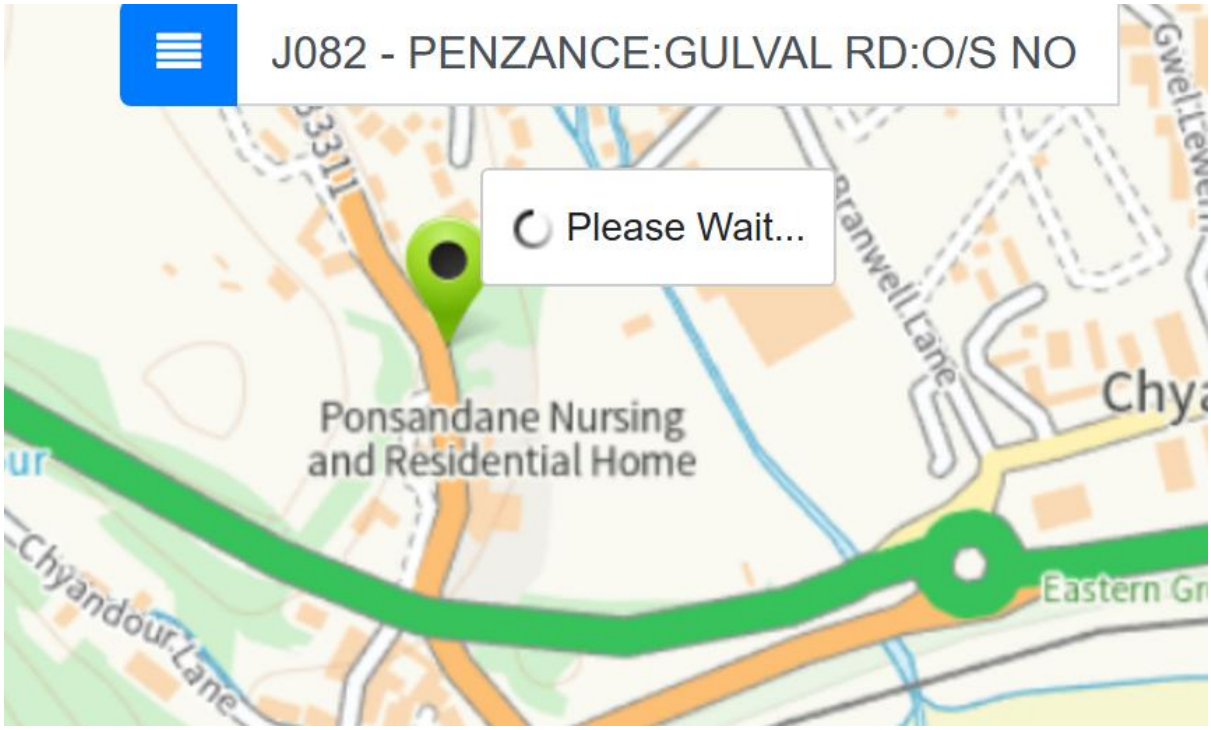

P108 - PENZANCE:ALVERTON:OPP PIF
Please Wait...
Alverton Road
Boswergy
Ivy Lane
Trenoweth Road
Lansdowne Close
Lansdowne Road
Penpons Close
Allotments
Alverton

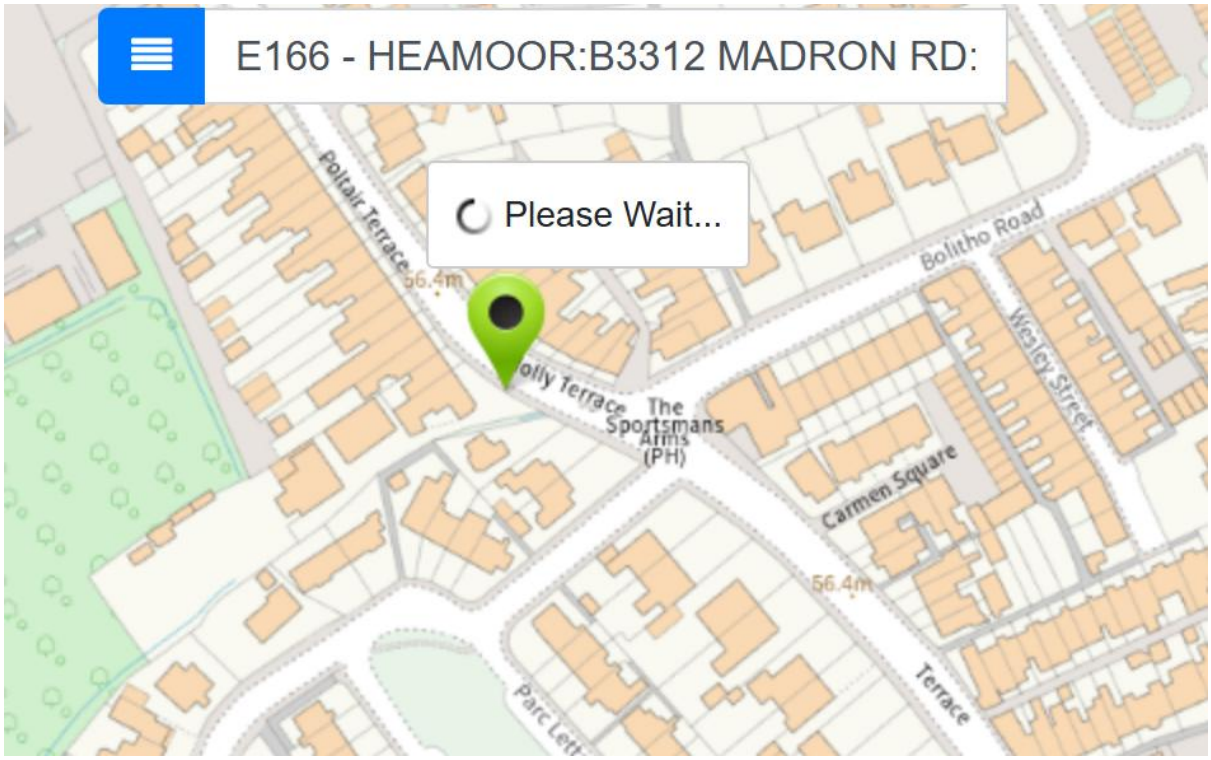

M080 - PENZANCE:MORRAB RD:PARK
Please Wait...
Buriton Row
North Parade
Park Corner
Penzance School of Art
Other Sports Facility
Tennis Court
Tennis Court
Penlee Memorial Park
Public Park Or Garden
Play Space
Tennis Court
Playing Field
Morrab Road
Morrab Place
Parade Street
Princes Street
Queen Street
Pengarth
Morrab Gardens

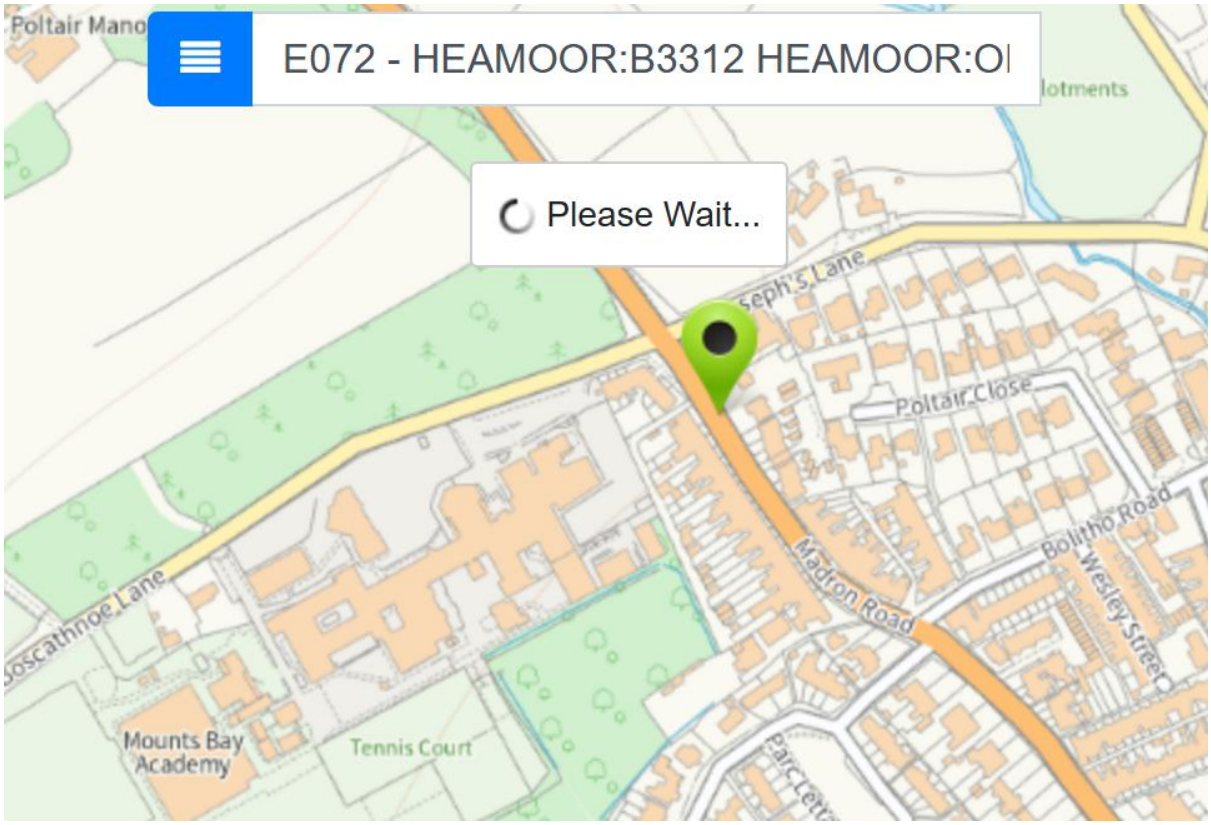

K156 - PENZANCE:PENWITH ST:O/S N
Please Wait...
St Michael's Street
St Phillip Street
St Dominic Street
St Mary's Street
Gwavas Street
Penlee Street
Penwith Street
Cemetery
Allotment Gardens
Leskinnick Terrace
Trewartha Terrace
Lescudjack Road
Albert Villas
Mount Street
13.7m

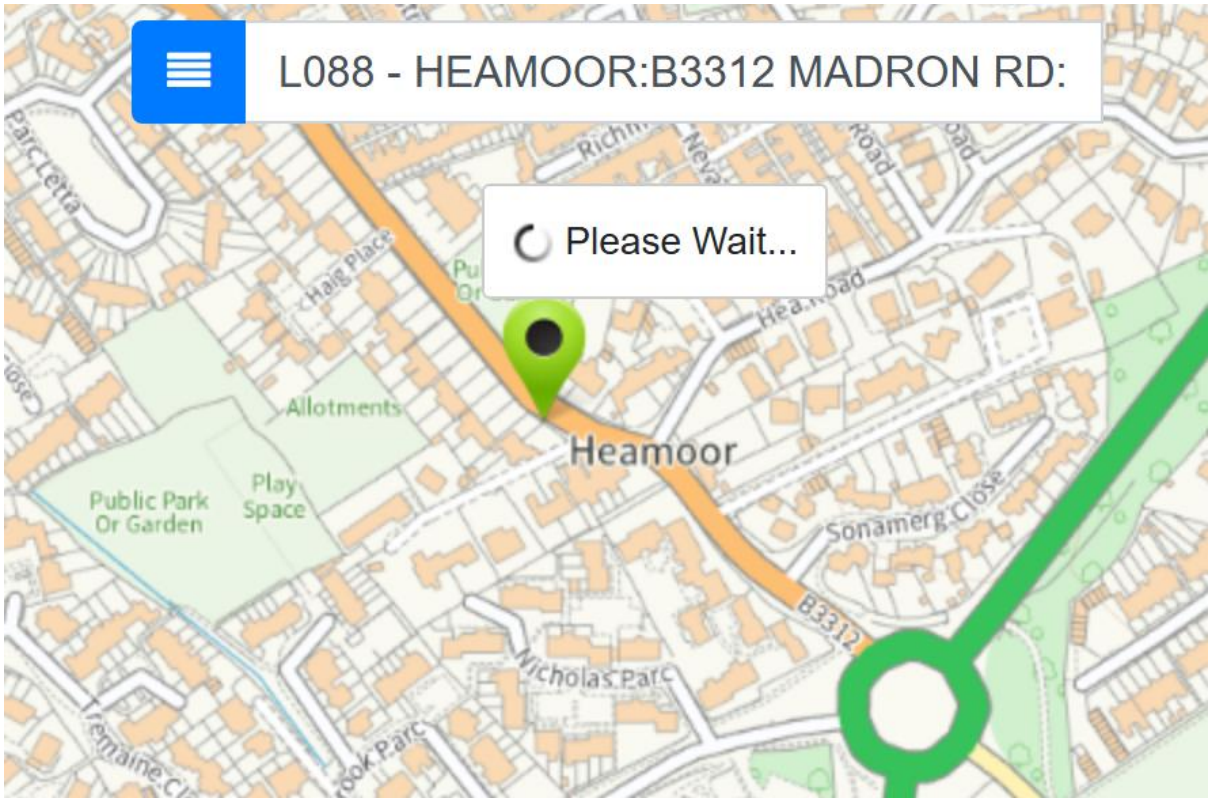

J096 - PENZANCE:GULVAL RD:JNT TRI
Please Wait...
19.5m
25.7m
25.9m
26.2m
21.5m
Ridgevale Lane
Chynoweth Gardens
Gulval School
The Old Workshop
13.4m
Green Lane Hill
17.8m
Trewarrack Road
El Sub Sta
Gwel An Porth


J160 - GULVAL:SCHOOL L:O/S TREVEA
Please Wait...
Gulval
St Gulval's Church
Cemetery


J082 - PENZANCE:GULVAL RD:O/S NO
Please Wait...
Ponsandane Nursing and Residential Home
Chyandour Lane
Eastern


E166 - HEAMOOR:B3312 MADRON RD:
Please Wait...
Poltair Terrace
56.4m
Bolitho Road
Wesley Street
olly Terrace
The Sportsmans Arms (PH)
Carmen Square
56.4m
Terrace


E072 - HEAMOOR:B3312 HEAMOOR:O
Please Wait...
Poltair Close
Madron Road
Wesley Street
Mounts Bay Academy
Tennis Court


L088 - HEAMOOR:B3312 MADRON RD:
Please Wait...
Allotments
Heamoor
Public Park Or Garden
Play Space
Sonamerg Close
B3312

PRODUCT DOCUMENTATION

EVOLIS VISION

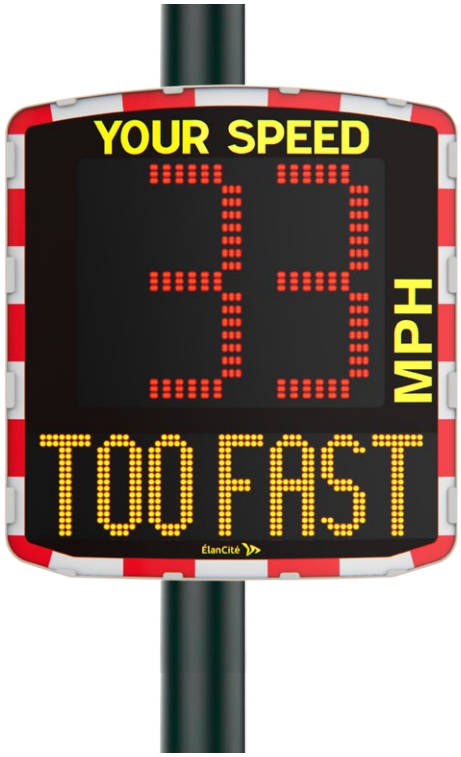
THE STATE-OF-THE-ART RADAR SPEED SIGN

ElanCity

www.elancity.co.uk

THE WORLD'S MOST FREQUENTLY CHOSEN MODEL

Accuracy, striking visibility, reliability in all conditions, easy to install, the EVOLIS Vision radar speed sign boasts a host of advantages that have made it an international benchmark: nearly 20,000 town councils have adopted it and there are over 45,000 units in operation worldwide.



1 An impactful display making it the most effective of radars

- Greater visibility meaning earlier driver awareness
- Customizable messages to match your priorities
- Accurate, long-range Doppler radar antenna (300 meters)

2 Connected radar for high-performance analysis

- Traffic data recorded in both directions
- A software package for analyzing your traffic data
- Various connectivity options

3 Durability and long-term reliability

- Extremely durable housing
- Robust front face
- Two-year parts and labour guarantee
- Extended warranty for your peace of mind

4 Simple, safe installation

- Easy installation built into the design
- Can be configured directly on the appliance
- Four power supply modes to suit sites of all kinds
- Lightweight: only one person needed for installation or relocation

TESTIMONIALS FROM OUR CUSTOMERS

I have to say that we are absolutely delighted with the new device and we have had lots of positive comments from residents who are also very impressed. I am sure we will be placing a further order with you in the New Year.

Mr Craig Bowne, Councillor to Alderley Edge Parish Council (Cheshire)

A STRIKING DISPLAY, MAKING IT THE MOST EFFECTIVE RADAR

Accurate is fine, but unmissable is better. With a 300 meters vehicle detection range and optimum visibility up to 250 meters, EVOLIS Vision is considered the best performing and most safety-inducing radar on the market!

Dual display: speed figures and warning messages

EVOLIS Vision has 2 displays: **the first displays the speed detected by the Doppler antenna.** The speed display is made up of 3 rows of LEDs: a maxi format and a high resolution which greatly increase visibility and the psychological impact on the driver.

EVOLIS VISION'S VISUAL PERFORMANCE VERSUS ITS COMPETITORS

EVOLIS Vision: 3-row LEDs

Competitor's product: 2-row LEDs

Competitor's product: 1-row LED

The second display, at the bottom, can be used to display text that can be fully customised according to speed. EVOLIS Vision also has a wide range of pre-recorded messages and pictograms.

With its **large matrix** (16 x 64 cm), the EVOLIS Vision radar's text display is a major asset toward achieving greater impact on motorists and inciting them to slow down.

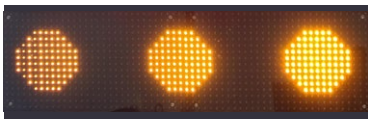
Discover also EVOLIS Mobility!

The version without text display of EVOLIS Vision (with a screen-printed text).

Contact us for more information!

Customizable messages according to your priorities

EVOLIS Vision adapts to the stretch of road you want to make safe. The “Full LED” text display matrix lets you customize messages to suit specific locations or periods, e.g., protection of pupils at school break-up times. You can also alternate two or three flashes with a special message to grab the attention of drivers used to driving past the display without noticing. Outside these specific times, standard messages are resumed.

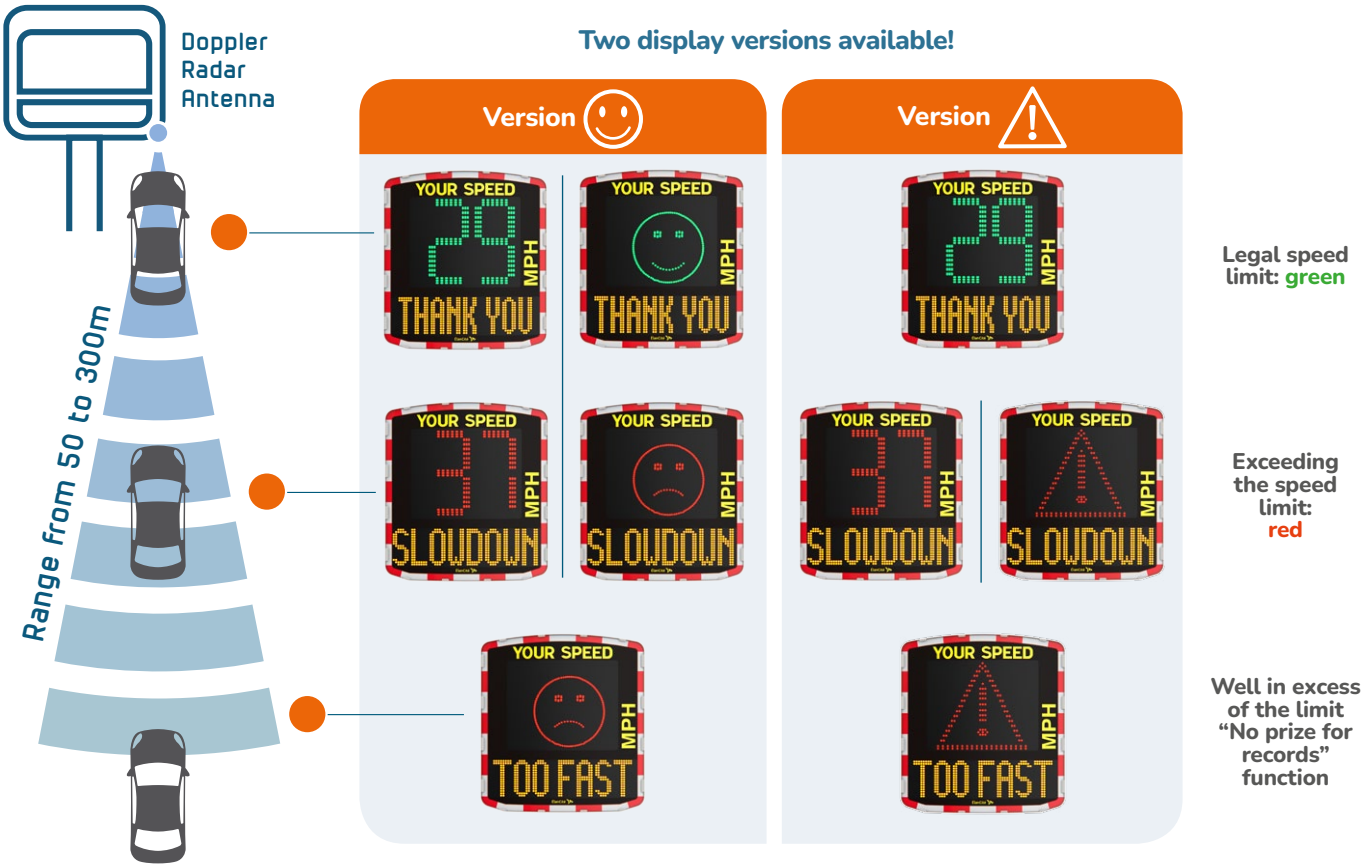


Accurate, long range Doppler radar antenna

This tried-and-tested technology used in our radar speed displays enables us to guarantee accurate detection at ranges up to 300 meters, a wide detection angle of 33° and an accuracy of +/- 1%. **The longer the detection range**, the more the driver comes face-to-face with their speed and **the bigger the radar’s effect!**

The different interactions between EVOLIS Vision and the motorist

The two-tone display, refreshed every second, ensures a strong impact on the motorist. It is green when the speed limit is respected, and red when it is exceeded.



A CONNECTED RADAR FOR HIGH-PERFORMANCE ANALYSIS

The EVOLIS Vision radar doesn't stop at warning drivers. The integrated software lets you manage your equipment with your own resources and record and analyze traffic data in your community.

How do you communicate with your radar?

Through your PC, you can exchange data with your radar via USB cable (included) and Bluetooth®. You can also connect to your radar via **your tablet or smartphone under Android/iOS.**

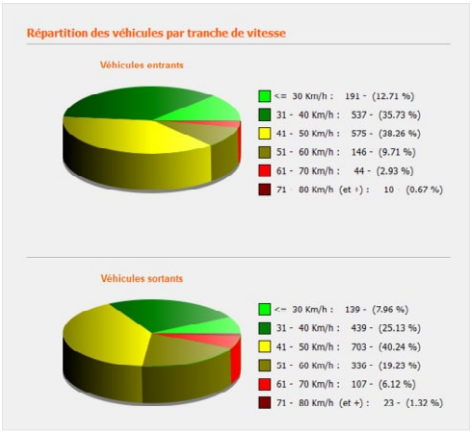
Spy mode: the smart way to analyze data

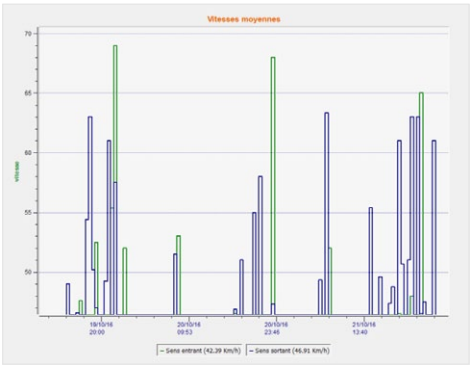
The extremely useful "spy" function lets you **compare the radar unit's traffic data** in the on and off modes. With this system, the EVOLIS Vision radar doesn't display speeds but still records the traffic data.

A software suite to analyze your traffic data and prove the effectiveness of the radar speed sign

Configure your radar easily and retrieve its recorded data with our software package (unlimited access license): number of vehicles time stamped to the nearest second, speed in both directions, average and maximum speeds, etc.

It can also output your data in graphic form: pie charts, diagrams, graphs, etc., **providing you with precious information on road safety in your town or village**. All the data can be exported as an Excel, CSV, or PDF file.





Discover Option Connect

The Connect box provides the EVOLIS radar with remote connectivity using the 4G network. Easy to implement, it is installed directly inside the unit by the user. The Connect box offers easy management of your EVOLIS radar as well as unparalleled practicality when managing your statistical data.

With its «all-inclusive» subscription, you can remotely access all your statistical data settings and the health status of your radar through our dedicated web platform.

DURABILITY AND LONG-TERM RELIABILITY

From Canada to New Zealand, across Europe, installations all over the world are proof that EVOLIS Vision radars are designed to work long term in any climatic condition.

Extremely durable housing

Made of polycarbonate-reinforced ABS resin, the one-piece housing guarantees perfect weatherproofing and protection of the components.
There are no screws to go rusty. The full-core anti-UV treatment ensures maximum service life.

Robust front face

Designed in polycarbonate and treated with an anti-reflective coating, it offers better visibility in all conditions.

Slightly curved, it protects the LEDs from all projectiles.

A 2-year warranty and a dedicated support team

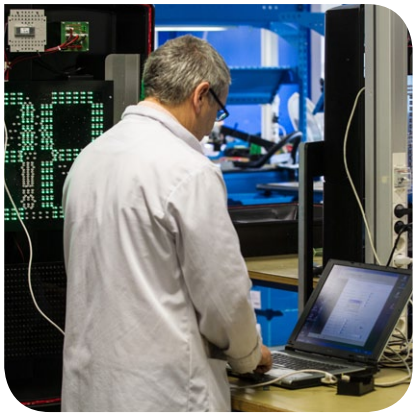
The return rate of our radars under guarantee is less than 1%.
In case of malfunction (except vandalism), we proceed with you to the diagnosis by phone and bring you the necessary support for the repair. Our team of specialists assists you with installation and use: telephone talk-throughs or onsite training are both possible.

An extended warranty for your peace of mind

At the end of the 2-year warranty period, we offer you a warranty extension including:

- The repair of the equipment in the event of a malfunction, including parts, labour and transport
- Updating of on-board firmware and user software
- Telephone assistance to answer your questions regarding the use of the device.

Thanks to this warranty extension, you can rest assured that your Radar Speed Sign will remain a constant ally in reducing speed on your roads.



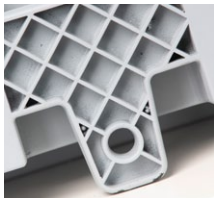
A SIMPLE AND A SAFE INSTALLATION

The EVOLIS Vision is cleverly designed to enable installation and relocation in a matter of minutes on any existing support structure by a single member.

Easy installation built into the design

Delivered pre-configured and ready to go, the EVOLIS Vision has been designed to make it easy to install and use:

- Weighs only 9.2kg, allowing easy manipulation without heavy equipment
- Large detection angle of 33° for installation without orientation of the radar
- Universal mounting bar
- Specific supports that fit any type of installation
- Able to be secured by padlock for added security



Setting up: an interface for pre-selecting speed limit

Configuration directly on the radar:

Where to place them for maximum effect?

To achieve significant speed reductions, drivers need to be reminded of their speeds for as often as possible. Town entrances, village main roads, approaches to schools - for maximum effectiveness, the best positions are:

- Locations visible from a substantial distance (50 to 200 meters)
- Locations providing a clear line of sight to allow the antenna to detect individual vehicles across a longer distance (avoiding trees, crossroads, car parks, etc.).

FOUR POWER SUPPLY MODES FOR ADAPTABILITY TO ALL LOCATIONS!

Two versions of EVOLIS Vision with four low-energy power supply modes are available for adaptability to all your town's situations and all climatic conditions.

SOLAR PACK

POWER	AUTONOMY
Batterie power Batterie version with external charger	A charge life of **1 to 2 weeks** (depending on traffic) Upgradeable to solar-powered
AND / OR	
Solar version	**Guaranteed autonomy** - 100 watts: up to **7,000** vehicles/day - 150 watts: up to **12,000** vehicles/day

HYBRID PACK

POWER	AUTONOMY
Public and/or **permanent lighting**	**Complete autonomy** with a minimum of 5 h of continuous public lighting
AND / OR	
Hybrid mode (electric and/or solar)	**Complete autonomy** EVOLIS Vision can be fitted with a solar panel at a later date

TECHNICAL CHARACTERISTICS

DISPLAYS	**Speed Digits**	3 digits (0 to 199) Dimensions: 380 x 450 mm Colour: green / amber / red Visibility: 3-LEDline thickness
	Smileys	Colour: green / red Dimensions : 300 x 300 mm
	Message/Graphic display (excluding EVOLIS Mobility)	Dimensions: 160 x 640 mm (H x W), 1 line of 8 characters / 2 lines of 11 characters Colour: amber Programmable messages – text and pictograms
	LEDs	OSRAM C.M.S high-luminosity, ultra-low consumption Service life > 100,000 hours
	Photosensitive cell	High-precision sensor for adaptation to the light
DOPPLER RADAR ANTENNA	**Range**	Up to 300 metres
	Accuracy	within 1%
	Angle of detection	33 degrees
	Frequency	24.200 GHz
TRAFFIC STATISTICS	**Analysis**	In both traffic directions (incoming/outgoing)
	Data	Average and maximum speeds, number of vehicles, time stamps, percentiles (V30/V50/V85)
	Memory	16 Mo, 5 million vehicles recorded
	Operation	With the software package. Output exportable in Excel, CSV, or PDF files.
SETTING UP	**Local**	USB and Bluetooth®® (PC or Android/IOS mobile appliance with mobile app) Prerecorded speed bands with selection interface
	Remote	4G modem with Web interface (operational status of appliance and statistical analysis)
HOUSING	**Dimensions**	710 x 770 x 160 mm (W x H x D), with two battery slots
	Weight	9.2 kg (excl. batteries)
	Material	ABS resin, anti-UV, one-piece injection moulded body
	Colour	Grey, through dyed
	Ingress protection	IP65
	Security	Lock and specific key, also provision for padlock
	User access	External access to batteries, speed change interface, and USB port. Secured by two locks
FRONT FACE	**Material**	Polycarbonate with nonreflective surface
	Decoration and text	Regulatory red and white border - Silkscreened text “Your speed” Reverse silkscreen printing
	Shape	Convex for optimum protection against projectiles
POWER SUPPLY	**Battery**	Lead-acid 12V, 22Ah Weight: 6.2kg Dimensions: 181 x 76.2 x 167mm (L x W x H)
	Charging by solar panel	100 watts Monocrystalline high-output cells Dimensions: 806 x 680 x 35 mm (L x W x H) Smart charging management
	Charging from street lighting or grid	Internal power 220 V Smart charging management Integrated protection fuse
COMPLIANCE	**European standards**	Directive RED 2014/53/EU Directive RoHS 2011/65/EU Directive WEEE 2012/19/EU

ElanCity

A COMPREHENSIVE RANGE FOR ROAD SAFETY AND LOCAL COUNCIL COMMUNICATION

Drawing on its expertise in radar speed displays, Elan City capitalizes on its know-how and flair for innovation by expanding into other areas of display, including municipal information and road traffic management. The priority remains the guarantee of reliability, durability, toughness, and ease of installation and use.

EVOLIS®

The most effective radar speed display in the world, providing the highest efficiency

- Significant, lasting decrease in speeding
- Recording of traffic statistics in both directions
- Bluetooth® and/or 4G communication
- Available with solar and/or electrical power supply

EVOLIS Vision

EVOLIS Mobility

EVOFLASH

A beacon to boost your existing road safety signage

- Triggering on vehicle detection and/or overspeed
- Adaptable to all support posts: universal fastening and solar self-sufficiency

EVOCITY

The only electronic information display that can run on 100% solar power or public lighting

- Excellent reading quality in all conditions of light
- Versatile: can be relocated

Find out more by consulting your assigned sales representative

ElanCity

A TEAM LOCAL COUNCILS HAVE LEARNT TO COUNT ON

Elan City has been designing, manufacturing, and distributing products to fulfil the needs of local authorities for over 20 years. We are first and foremost a team focused on customer satisfaction, with a strong commitment to tackling issues that lead to improvements in local road safety.

Founded in 2005

50 staff

Nearly 20.000 towns and villages equipped and nearly 50.000 units in operation

Elan City, the safety and security partner

It doesn't matter whether you are a municipality, a district council, a county council, or a big city: our experts with their solid experience in the trade (7 years on average) will bring you unmatched effectiveness in the materialization of all your projects.

The Children's Trust

WILLIAMS RACING

Many private sector enterprises also trust us for securing access to their production sites. EVOLIS can be adapted to all situations.

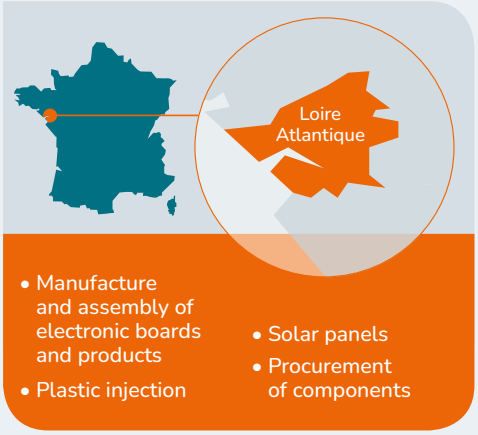
Cambridgeshire County Council

The Highland Council
Comhairle na Gàidhealtachd

100% high-quality French manufacture

FABRIQUÉ EN FRANCE

All our second-tier suppliers are also French and ISO 9001 certified. By operating stringent checks at each stage, we are able to guarantee you consistent optimum quality.



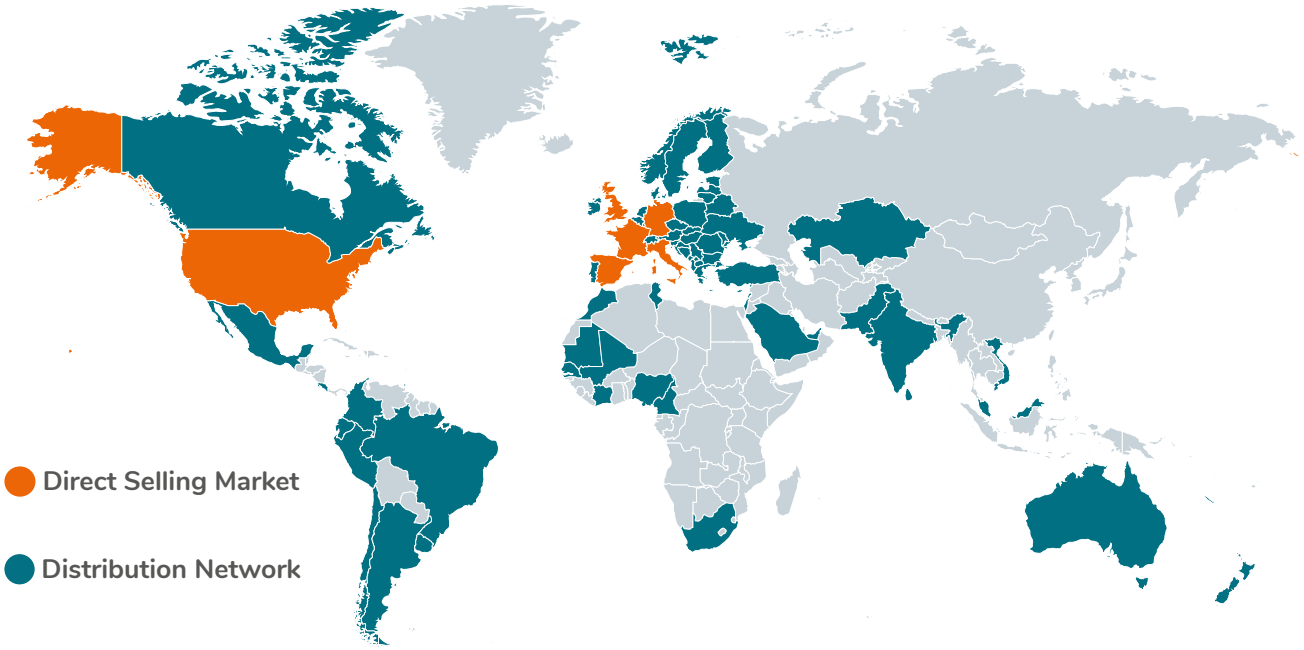
Furthermore, we are fully committed to complying with European environmental regulations. Our products comply with RoHS and WEEE directives, ensuring environmentally friendly and responsible management of electronic waste.

Additionally, a specialized waste treatment channel is in place to guarantee their recycling in accordance with environmental standards.

RoHS COMPLIANT

A PRESENCE ALL OVER THE WORLD

Élan Cité is the founding entity of Elan City Group. Today, Elan City has 5 European subsidiaries, 1 subsidiary in the United States and a global presence thanks to a distribution network of more than 40 distributors.



- **Elan City Germany**
  Savignystraße 43
  60325 Frankfurt am Main
  info@elancity.de
- **Elan City Spain**
  C/Velazquez 80, 5 Izq
  28001 Madrid
  ventas@elancity.es
- **Élan Cité France**
  12 route de la Garenne
  44700 Orvault
  contact@elancite.fr
- **Elan City Italy**
  Corso Vittorio Emanuele II, 71
  10128 TORINO TO
  vendite@elancity.it
- **Elan City USA**
  450 7th Avenue
  New York, NY 10123-1591
  sales@elancity.net
- **Élan Cité Export / Distributors**
  12 route de la Garenne
  44700 Orvault
  export@elancite.fr

Headquaters:
Orvault, region of Nantes, France

Expertise hailed in over 50 countries

ElanCity

Wilberforce House
Station Road
LONDON NW4 4QE
+44 20 3936 0920
sales@elancity.co.uk
elancity.co.uk

Discover EVOLIS Vision on video by flashing this QR Code!

Elan City - June 2024 - © Elan City - Adobe Stock