**Report No. 43/24**
**National Park Authority**

## Report of Performance and Compliance Officer

---

## Subject: Record Management and Retention Policy

**Purpose of Report**
To ask Members to approve the Record Management and Retention Policy.

**Background**
The Authority has been undertaking activities in support of improved record management, including

- Updating documentation to meet accountability requirements under UK GDPR/ Data Protection Act 2018. Management Team approved an updated retention schedule on 1/10/24.
- Responding to impact of change programmes in terms of introduction of Microsoft Teams/ Sharepoint and Authority reorganisation

As part of these programmes of work, it was recognised that a new policy needed to be developed focused on record management and retention to sit alongside the retention schedule.

The Policy sets out the:

- Legal framework the Authority needs to comply with for record management and principles for good record management
- Requirements for creating and storing paper and digital records
- Requirements for access and sharing records, in particular with third parties, contractors and partner organisations
- Requirements for retention and disposal of records

From our record management activities there was a recognition for a need to strengthen accountability in terms of roles and responsibilities. Under the policy the Chief Executive is identified as the Senior Information Risk Owner, and members of Management Team are identified as Authority's Information Asset Owners.

A Proforma template will be included in the Appendix of this Policy that Managers will be able to use for their departments to note where to Save/ Store Items.

The policy has been reviewed by Data Protection Officer. Members, Staff and Management Team have been provided with opportunity to provide feedback on the draft policy.

**Financial considerations**
Non-compliance with this policy could open the Authority up to data breaches with financial implications in terms of fines and cost of remedial action. Effective record management can also make it easier if breach or cyber incident occurs to manage the incident.

Effective record management and retention practices can help

- Reduce burden when Freedom of Information, Environmental Information and Subject Access Requests are received.
- Help teams to be more efficient, reducing time spent locating records.
- Help reduce pressures and costs tied to digital storage.

Grant funded projects often have specific requirements placed on them in terms of retention period.

**Risk considerations**
Effective record management can help mitigate risks in terms of data protection breaches and make it easier to respond to Freedom of Information, Environmental Information and Subject Access Requests and impact of Cyber Security Incidents. It also means that we have the documents needed available if we face legal claims or are audited by external grant providers.

From our record management activities there was a recognition for a need to strengthen accountability in terms of roles and responsibilities. Under the policy the Chief Executive is identified as the Senior Information Risk Owner, and members of Management Team are identified as Authority's Information Asset Owners.

**Compliance**
This policy supports the Authority to comply with UK GDPR and the Data Protection Act 2018, Freedom of Information Act 2000, Environmental Information Regulations 2004 and Code of Practice on the Management of Records issued under section 46 the Freedom of Information Act 2000

Erasing, destroying or concealing information with the intention of preventing its disclosure following receipt of a Freedom of Information, Environmental Information or Subject Access request is a criminal offence

When looking at a records lifecycle all those involved must consider the legal and regulatory environment specific to a department's area of work.

The Authority must be mindful of the implications of current public inquiries to its record keeping and retention practices. This includes considering the Inquiry's Terms of Reference, taking account of documents that may be relevant to the Inquiry and securely retaining and keeping them accessible in case they need to be disclosed to the Inquiry.

**Equality Duty**
The policy will support the effective management of special category data.

**Section 6 Duty**
Effective record management and retention can help reduce carbon emission footprint of our digital storage. The policy also supports reduction in creation of new paper records.

**Welsh Language**
This policy applies to records held in Welsh or English.

**Recommendation: Members are asked to approve the Record Management and Retention Policy**

(For further information, please contact Mair Thomas, Performance and Compliance Officer)

Consulted/engaged with: Management Team, Data Protection Officer, Staff and Members.

Polisi Corfforaethol
Corporate Policy

# Pembrokeshire Coast National Park Authority

## POL_IG4 Record Management and Retention Policy

| Version | Active Date | Document Owner | Internal/ External |
|---|---|---|---|
| 1 | Draft | Chief Executive (SIRO) | Internal |

Please note: Policy Control Sheet is at the end of the document. Policy document is uncontrolled once printed. Please refer to the Authority's Intranet site for up-to-date policy.

### Does this Policy relate to me:

- This policy relates to all staff, volunteers, Members, partner organisations, contractors who handle records or data on behalf of the Authority

### Quick Reference - Key Policy Messages:

The Policy sets out the:

- Legal framework the Authority needs to comply with for record management and principles for good record management
- Requirements for creating and storing paper and digital records
- Requirements for access and sharing records, in particular with third parties, contractors and partner organisations
- Requirements for retention and disposal of records. The retention schedule should be read alongside this policy
- Pro forma Template – Where to Save/ Store Items included as an Appendix of this document

## Contents

## 1. Policy Statement

1.1 Pembrokeshire Coast National Park Authority (the Authority) recognises that its records are an important public and corporate asset, and are a key resource required for effective operation and accountability.

1.2 The Authority's approach set out in this policy aims to support compliance with the following key data protection principles within the UK GDPR and Data Protection Act 2018:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (Security)
- Accountability

1.3 Failure to comply with the above may leave the Authority open to substantial fines and place people's data at risk.

1.4 To work effectively the Authority needs to

- Create and capture authentic, reliable and timely records
- Demonstrate accountability and transparency in decision-making at all levels

1.5 The Public Ombudsman for Wales has identified that good record management can be achieved by following a number of key principles which the Authority will implement in its approach to record management:

- Knowing what records are held where and who is responsible for them
- Having effective records management systems in place
- Keeping records accurate and up to date
- Ensuring records are comprehensive, relevant but not excessive
- Creating reliable records
- Ensuring all staff now what is expected of them
- Storing records securely so they can be readily accessed when needed.[1]

1.6 The Authority's record keeping approach should support the effective administration of Freedom of Information, Environmental Information Regulation and Subject Access Requests.

[1] Good Records Management Matters – Public Services Ombudsman for Wales, 2022

1.7 The Authority approach will ensure that it has necessary documentation in the event it receives a challenge or complaint.

## 2. Aim of Policy

2.1 To ensure the Authority has in place effective record management and retention practices that comply with relevant legislation and support effective business administration.

2.2 Setting out clear expectations for staff and others on record management and retention.

## 3. Scope of Policy

3.1 This policy applies to all the records created or held by the Authority, in any format, however they are stored (e.g. IT system/database, cloud storage, electronic file storage, filing cabinet/shelving, Office 365 - including e-mail and Teams).

3.2 The retention schedule which is a separate document should be read alongside this policy.

## 4. Definitions

4.1 Records are defined by the International Standard Organisation as ‘‘Information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business.’

4.2 Records can be in any format including, but not limited to, physical, digital and audio visual.

4.3 Records management involves the systematic management of all records and the information they contain throughout their lifecycle. The guiding principle of records management is to ensure that information is available when and where it is needed, in an organised and efficient manner, and in a well-maintained environment.

4.4 ‘Personal data’ is defined in the UK GDPR as any information relating to an identifiable person who can be identified directly or indirectly by referring to an ‘identifier’. In practice, a wide range of identifiers will constitute personal data, including names, addresses, unique reference numbers, online identifiers and narrative about a person.

4.5 The UK GDPR also defines special categories of sensitive personal data:

- Racial or ethnic origin
- Political opinions

- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Health
- Sex life or sexual orientation

4.6 Criminal convictions data is specified as a separate category in the UK GDPR and is defined as information about criminal allegations, proceedings or convictions.

4.7 Metadata is **data that describes other data**. It's like a label that provides information about a piece of data, such as its author, date created, file size, and more. For example, the metadata for a document might include the title, author, and date it was last modified.

## 5. Legislation

5.1 UK GDPR and the Data Protection Act 2018

5.2 Freedom of Information Act 2000

5.3 Environmental Information Regulations 2004

5.4 Code of Practice on the Management of Records issued under section 46 the Freedom of Information Act 2000

5. 5 **Erasing, destroying or concealing information with the intention of preventing its disclosure following receipt of a Freedom of Information, Environmental Information or Subject Access request is a criminal offence.** This offence can apply to both a public authority and to any person who is employed by, is an officer of, or is subject to the direction of the Authority.

5.6 Communication carried out relating to Authority business where records are produced such as e-mails, Microsoft Teams Posts/Chat function or phone calls recorded via customer services may be subject to above disclosure requests. At all times when using e-mail or chat functions staff and Members should be accurate in their recording, respectful of others, and record only what is necessary.

5.7 **The Authority must be mindful of the implications of current public inquiries to its record keeping and retention practices. This includes considering the Inquiry's Terms of Reference, taking account of documents that may be relevant to the Inquiry and securely retaining and keeping them accessible in case they need to be disclosed to the Inquiry.**

5.8 Additional Guidance:

- Good Records Management Matters – Public Services Ombudsman for Wales
- ICO – Record Management and Security
- Records Management Society of Great Britain – Retention Guidelines for Local Authorities

## 6. Roles and Responsibilities

### 6.1 Senior Information Risk Owner (SIRO).

The Authority's SIRO is the Chief Executive Officer. The SIRO is responsible for information risk within the Authority and must ensure that effective records management policies and processes are in place.

### 6.2 Authority's Information Asset Owners

The Authority's Information Asset Owners are members of the Authority's management team. They are responsible for

- All information processed within their department or processed in partnership with another department
- Management of their department's records in accordance with this policy
- Understanding what information and records are held, how they are used and transferred, who has access to them and why, to ensure compliance with legislation and minimise the level of risk
- Ensuring that all those in their department who handle records are aware of, and practice, good records management
- Ensuring local procedures are developed and implemented relevant to the work of their department to ensure compliance with this policy. This includes completion of Pro forma Template – Where to Save/ Store Items for teams within their department.
- Ensuring that records for their department are suitably moved from temporary storage (for example staff's Microsoft OneDrives) into the appropriate storage platform for official record keeping
- Ensuring information that their department has created, received or been responsible for in the course of work remains accessible when a member of their department leaves their role or the Authority
- Working to ensure their department sets aside time periodically to review files and confirm data management is compliant
- Authorising records' disposal according to this policy and retention schedule
- Ensuring the Performance and Compliance Officer is notified in a timely manner of any changes needed to the records of processing, disposal of records register or retention schedule. Information Asset

Owners will be asked to review the Record of Processing for their service and Retention Schedule on annual basis to confirm it remains accurate and up to date.

- Ensuring that data protection impact assessments are completed when there are proposed changes to the processing and storing of records containing personal data
- Arranging for data sharing agreements to be put in place when their department is involved in sharing personal data records with third parties, other public bodies and partners. They are responsible for ensuring this is done before any data sharing takes place, including for any joint projects or work commissioned with external contractors and consultants
- Bringing to the attention of wider Management Team any record management concerns

### 6.3 Project Managers

Project Managers are responsible for the following:

- Taking responsibility for managing project information from the start to the finish of a project
- Checking with Data Protection Officer to see if a data protection impact assessment is needed for the project and completing one if it is required before personal data is processed by the project
- Liaising with IT team to close down Microsoft Teams (and private channels), ensuring that business and project information is migrated to a suitable place for continuing retention
- Transferring evidence of major projects to Corporate digital archive

### 6.4 Contract Managers

Contract managers are responsible for ensuring that third parties and partner organisations understand their obligations in receiving, handling, storing, disposing and returning information while executing their contracts and agreements. They must ensure that due diligence is completed and appropriate data processing agreements are put in place with third parties and partner organisations.

### 6.5 All, employees, casual and agency workers, volunteers and contractors

Are responsible for

- Taking personal responsibility for the effective management and protection of information
- Creating full and accurate records of their work, inputting data and naming files in such a way that they can be easily accessed and understood by future colleagues

- Storing information in shared locations that are accessible to colleagues and partners who are authorised to access it
- Keeping sensitive and confidential information secure when not in use and not leaving it visible on an unattended computer or desk
- Retaining records until they have reached the end of their retention period as set out in the Authority's retention schedule
- Only destroying records after approval from the relevant Information Asset Owner, when records are no longer required and do not have ongoing corporate value
- Ensuring information they have created, received or been responsible for in the course of their work remains accessible when leaving their role or the Authority

6.7 **Members**

Members are responsible for complying with this policy when acting as a Member of the Authority, for example when dealing with confidential papers or information in an e-mail.

6.8 **Data Protection Officer**

Is responsible for

- Assisting the Authority to monitor internal compliance with data protection laws and Authority's data protection policies
- Informing and advising on data protection obligations, Data Protection Impact Assessments (DPIAs) and acts as a contact point for data subjects and the Information Commissioner's Office (ICO)
- Reviewing contracts and data processing agreements with data processors, third parties and partners to ensure they include relevant clauses in compliance with UK GDPR and Data Protection Act 20218

6.9 **IT Team**

Are responsible for supporting implementation of information and data security policies and procedures which are designed to hold records securely, ensure back-ups are taken, and protect data and information from internal and external threats. This includes implementing access permissions for F Drive and Microsoft Teams (Sharepoint).

6.10 **Performance and Compliance Officer**

Will support

- The co-ordination and periodic review of the record of processing, retention schedule, hard copy information asset register and disposal

of records register and request annual review from Information Asset Owners

- IT to carry out periodic audits to check compliance against the retention schedule and wider record management and retention policy to identify risk areas or areas for improvement

## 7. Overarching Records Lifecycle

7.1 Managing records effectively is essential to the efficient running of an organisation. Information must be proactively and consistently managed from creation or receipt, through active use, collaboration and maintenance, to disposal either by destruction or transfer to corporate physical or digital archive.

7.2 All Authority employees and those delivering services on its behalf are involved in creating, maintaining and using records and it is important that everyone understands how records are produced and retained in their service area.

7.3 Information created, received and maintained during business activities belongs to the Authority and must not be used for any activity or purpose other than the Authority's official business.

7.4 **When looking at a records lifecycle all those involved must consider the legal and regulatory environment specific to a department's area of work.**

## 8. Creating and Storing Paper Records

8.1 New paper records should only be created, where this is required for evidential, historical or legal purposes and a digital copy is not sufficient. The Authority's preference is for records to be maintained digitally wherever possible, and this should be embedded within operational processes for each team.

8.2 All paper records should be recorded on the hard copy information asset register. A clear filing and naming system should be in place. Paper records that contain personal data are required to be included in the Authority's records of processing with legal basis for processing included. This applies to all Authority sites.

8.2 Paper records that are not being added to anymore and that are not accessed on a regular basis must be reviewed against the retention schedule to consider if they need to be retained by the department or submitted to corporate archive library.

8.3 Paper records stored in corporate archive library will be controlled through a tracking system that documents their location and file movements. Paper records retrieved from the corporate archive library must be promptly returned after use.

8.4 Paper records should be stored in environmental conditions (stable temperature and humidity levels, adequate pest management and fire prevention are some examples) that protect them from deterioration. Paper legal documents identified as business critical as part of business continuity planning should be held in a fire resistant safe and where appropriate an authenticated digital scanned image held.

8.5 Printed paper duplicates of digital files for temporary reference should be disposed when no longer required. If they contain personal or sensitive information, they should be held securely until disposed of in confidential waste.

8.6 Paper records that are scanned with the intention of destroying the original should be scanned in such a way that the scanned image can be considered an authentic copy and quality of record is maintained.

## 9. Creating Digital Records

9.1 Information must be named in such a way that it can be easily found by others now and in the future – with clear, meaningful and consistent titles and descriptive metadata where required.

9.2 Protective Marking is a standardised method of highlighting which information needs additional care to protect it. All information created by the Authority is an official record, as a result there is no need to formally label official information. Some information with extra requirements for protection must be protectively marked with the descriptor – “Sensitive.” This only applies where sensitive information could have damaging consequences if lost, stolen or published, and the sharing warrants that handling requirements need to be reinforced. It is not necessary to protectively mark routinely shared work within a team.

9.2 Officers names should not be used to name a folder (the only exception is for HR and the labelling of personnel folders for individuals).

9.3 To be considered authoritative evidence, records must have the following characteristics:

- Authenticity: the record is what it claims to be and has not been tampered with. It can be relied on as evidence, for example in court
- Reliability: the contents of the record can be trusted as a full and accurate representation of the Authority’s activities
- Integrity: the record is protected against unauthorised changes, any changes are clearly indicated and have an audit trail
- Usability: the record can be found, used and understood as needed

9.4 A single version of the truth should be maintained, which is shared and reused between service areas. Avoid creating or keeping duplicates of information.

9.5 Processes will be developed to support this for corporate level documentation using Microsoft Teams for central document management and version control. Where all staff need access to corporate policies, procedures, forms, templates, meeting notes these will be published to the Corporate Document Hub on the staff intranet.

## 10. Storing Digital Records

10.1 Digital records that supports day-to-day business must be stored in either F Drive or SharePoint via Teams, unless there is an appropriate business system in place, for example APAS system is used by the Planning Team.

10.2 Legacy information will continue to be stored on the F Drive or Corporate Archive Drive. A record management project is exploring processes for a managed and consistent transfer of files from network drives to Teams/ SharePoint where appropriate.

10.3 OneDrive must not be routinely used to store Authority information, except for early drafts not ready to be shared more widely. Work information shared from an individual's OneDrive that is a corporate record must be moved to relevant Microsoft Team Folder (SharePoint) or F Drive for final storage. This is to support business continuity in terms of access to records created. Corporate records must not be stored on device hard drives, on portable media e.g. USB drives, or sent to personal email or cloud storage.

10.4 New business systems holding documents should be designed and configured to store records with metadata proportionate to their value. This supports their authenticity and integrity and helps each record to be understood.

10.5 Digital continuity must be considered for the systems and formats used to store digital records.

10.6 Photographs and videos where people are identifiable should be carefully stored with relevant metadata, with consent information cross referenced.

10.7 Information with retention periods over 10 years should be actively managed with consideration of whether they need to be retained at departmental or provided to corporate digital archive.

10.8 Where emails or chats form evidence of a decision, the decision should be captured outside of the messaging system and not kept in a personal inbox or private chat.

## 11. Access and Data Sharing of Digital Records

11.1 The IT team will apply access controls to Microsoft Teams and Folders on F Drive in consultation with the relevant Information Asset Controller. Designated owners of other systems must ensure that appropriate technical

and organisational measures are put in place to protect records from unauthorised access and accidental loss or destruction.

11.2 Users should share information from Microsoft Teams (SharePoint) via links. This helps to mitigate the risks from creating duplicates that need to be deleted and working with outdated information.

11.3 Users should attend IT provided Microsoft Teams Training to ensure that they are competent in use of links and managing access and restriction options when sharing them. When users are sharing links to documents they must make sure they are selecting the correct recipient(s) to avoid any potential data breaches.

11.4 Users must report data breaches immediately to the Data Protection Officer following the data protection breach procedure.

11.5 Where information is shared with or created by third parties, GDPR compliant contracts must set out what information is shared, how it can be used, how it should be handled and arrangements for its security and safeguarding. In line with the Data Protection Policy any data sharing must only be undertaken with the prior approval from the Authority's senior managers and in conjunction with the DPO. A suitable Data Sharing Agreement must be in place between both parties. This should be done before any data sharing takes place, including for any joint projects or work commissioned with external contractors and consultants.

11.5 External access to a Microsoft Team container or links to documents within a Team will be managed by approved e-mail list, managed by IT. It is recommended that Teams are set up specifically for collaborative projects that include external parties following the data sharing agreement being put in place.

11.7 Portable media containing personal data must be kept in lockable storage with access keys or codes also held securely.

## 12. Retention and Disposal

12.1 Information will be retained only for as long as it is required to support business need, legal obligations, for reference or accountability purposes, or to protect legal and other rights and interests

12.2 The Authority's retention schedule lists the records created by the Authority and the minimum amount of time they must be kept before destruction or whether they need to be kept permanently.

12.3 Information Asset Owners should provide authorisation for disposal. If the information has no current owner, the closest manager to the function is responsible for the decision, with advice from the Performance and Compliance Officer.

12.4 Disposal of information must be documented to provide evidence that the destruction took place in accordance with the retention schedule and with appropriate authorisation. Disposals should be logged in the disposal of records register.

12.6 **Information that is due for disposal, but related to an ongoing information request, legal proceeding, regulatory investigation, audit or public inquiry must not be destroyed until the matter, including any complaint or appeal, has been closed.**

12.7 Information that is trivial, needed for a limited period and not included on the retention schedule should be destroyed as soon as no longer required as part of routine housekeeping.

12.8 E-mails that are no longer required for operational purposes and are not the primary or only version of a record that we are required to retain in line with retention schedule should be deleted. If an e-mail is the only record of a decision or evidence of decision making process then it should be retained. This applies to both received and sent emails. E-mail trails may be required for auditing purposes, investigating complaints or as evidence in disputes with third parties.

12.8 Records representing the corporate memory of the Authority or of significant public interest that no longer have administrative value for a department should be offered to the Performance and Compliance Officer for storage in corporate digital/ hard paper library archive.

12.9 Records containing personal data or business sensitive data must be placed in confidential waste. Records awaiting destruction must be stored securely.

12.10 Documents stored on electronic systems should be deleted when no longer needed for business or retention purposes, including from back-ups.

## 13. Organisational and Technological Changes

13.1 Records management requirements must be routinely factored into ICT planning, procurement, implementation and decommissioning.

13.2 Digital continuity considerations should be included in Digital and Change processes. This includes ability to migrate data in order to ensure the completeness, availability and usability of information after the system has been decommissioned.

13.3 Data Protection Impact Assessments should be carried out to assess any record management or disposal risks and any mitigations required.

## 14. Skills Development and Learning

14.1 As all Authority employees and those involved in delivering the services on its behalf are involved in creating, using, and maintaining records it is vital that

everyone understands their records management responsibilities as set out in this policy.

12.2 Managers should as part of induction process provide overview of record management processes for their department to new starters. They will provide new starters with a copy of the completed Pro forma Template – Where to Save/ Store Items for their department or team.

12.3 Additional checklists and supporting guidance will be developed where required to support implementation of this policy.

12.4 All IT users should attend IT provided Microsoft Teams Training to ensure that they are competent in use of Microsoft Teams (Sharepoint) and managing and sharing records via this system.

12.5 Briefings will be provided to teams on request and regular reminders on records management topics shared through corporate communication channels.

## 13. Monitoring and Assurance

13.1 SIRO and Data Protection officer will monitor overall compliance with this policy.

13.2 Information Asset Owners will bring to the attention of wider Management Team any record management concerns.

13.3 Data breaches are monitored alongside response times for responses to Subject Access Requests, Freedom of Information Requests and Environmental Information Regulation Requests.

13.4 The Performance and Compliance Officer will work with IT to carry out periodic audits to check compliance against the retention schedule and wider record management and retention policy to identify risk areas or areas for improvement.

13.5 Data Protection, record keeping and cyber security risks will be monitored via risk register and tested via internal audit programme

13.6 This policy will be reviewed on a three year cycle or earlier to respond to legislative or organisational changes relating to record management.

## 14. Related Policies

14.1 Retention Schedule

14.2 Data Protection Policy

14.3 ICT User Policy

14.4 Information and Data Security Policy

14.5 Homeworking and Hybrid Working Policy

14.6 CCTV Policy and Register

14.7 Publication Scheme

14.8 Data Breach Procedure

## Appendix – Pro forma Template – Where to Save/ Store Items

Note: A word version of this template will be made available in the Operational Procedure and Template section of the Corporate Document Hub for teams to download and edit.

**Pro forma Template – Where to Save/ Store Items**

[Note: will be added to approved policy]

## Policy Control Sheet

### Change Level

| Change Level | Tick |
|---|---|
| Minor editorial/ accuracy changes | |
| Change requires Management Team Approval Only | |
| New Policy or Change requires NPA Approval / People Services Committee Approval | ✓ |

### Consultation

| Group | Date |
|---|---|
| Management Team | 6/8/24 |
| DPO | 31/7/24 |
| Staff and Members | 30/8/24 -24/9/24 |

### Assessments

| Assessment – If Applicable | Date |
|---|---|
| Integrated Assessment – Full | N/A |
| Integrated Assessment – Policy/ Procedure Review | N/A |
| Data Protection Impact Assessment | Wider DPIA is being completed on record management related to Sharepoint and sharing of data, this policy will feed into this DPIA. |

### Approval

| Approved by | Name | Date | Signature |
|---|---|---|---|
| National Park Authority | | | |

### Version History

| Version | Active Date | Summary of Changes |
|---|---|---|
| 1 | | New record management and retention policy. Updated lines of responsibilities and takes account of changes to organisational systems. |

### Review

| Version | Active Date | Document Owner | Review Date Trigger |
|---|---|---|---|
| 1 | | Chief Executive Officer (SIRO) | |

### Publication

Policies must be co-ordinated through the Performance and Compliance Team, for compliance, auditing, and control purposes. Please send all new or reviewed policies

once approved to mairt@pembrokeshirecoast.org.uk for formal publication of policy to staff, Members, volunteers and where required on the Authority's website.

| Publication | Date |
|---|---|
| Published on Sharepoint Corporate Policy Hub | |
| External Policy – Published on Website: HTML | |