Report of Data Protection Officer

Subject: Data Protection Policy

Purpose of the Report

This report seeks approval of the Authority's Data Protection Policy.

Introduction

The Authority's Data Protection policy has been reviewed by the Authority's new Data Protection Officer as part of a review of Authority's key documents relating to Data Protection.

The need to review the Data Protection Policy was also identified by the Authority's internal auditors as part of their ICT Review of Cyber Security. They recommended that the Data Protection Policy be re-written to provide a concise and clear explanation of how the Data Protection Act impacts on the Pembrokeshire Coast National Park Authority and for the policy to be updated to reflect changes to Data Protection Legislation and Regulations following UK withdrawal from the EU.

The policy went to Leadership Team for comment on the 9/8/21 and staff and Members had the opportunity to provide feedback and comments on the revised policy during 6-25th of August. These comments and responses were reviewed by the DPO and Performance and Compliance Co-ordinator.

Financial Considerations

Breaches of this policy could lead to external action against the Authority, including the issuing of financial penalties by the Information Commissioner's Office.

Failure to comply with this policy could lead to loss of essential business information and inhibit delivery of core services and functions of the Authority. Costs could arise from remedial actions to deal with breaches and security issues.

Risk Considerations

There is the potential for financial, safety, legal and reputational impact arising from the effectiveness of complying with data protection legislation.

The Authority is increasing its use of digital technology in how it operates which can increase risks in this area.

A clear policy, training and strong and active leadership is part of managing the risks. Tools such as Data Protection Impact Assessments can assist the Authority in managing its risks. The Authority has also appointed a Data Protection Officer to provide oversight of data protection compliance.

Compliance

This policy plays a central role in ensuring the Authority complies with Data Protection legislation and regulations.

Human Rights/Equality issues

This policy includes reference to the collection of Special Category Data and notes that any processing of this data must only be carried out with the explicit consent of the data subject. In order to fulfil the Authority's Equality Duties under the Equality Act 2010 the Authority will collect and process equality monitoring data from applicants, employees and some service users. Data subjects will be made aware that this is the reason why the data is being collected and how the data is stored, accessed, used and reported.

Welsh Language

The Data Protection policy will be translated into Welsh.

Recommendation

Members are asked to consider and approve the Data Protection Policy

(For further information, please contact Sarah Burns, Data Protection Officer)

Pembrokeshire Coast National Park Authority

POL_006 **Data Protection Policy**

Parc Cenedlaethol Arfordir Penfro
Pembrokeshire Coast National Park

External and Internal Policy

Review

Version	Effective Date	Document Owner	Review Date Trigger
3	(Insert date once approved)	PCNPA Data Protection Officer	Every 3 years. Legislative/ organisational changes. Security risk changes.

Target Audience

All employees, Members, volunteers, contractors, consultants or partners of the Authority who have access to any personal data held on behalf of the Authority.

Consultations

Group	Date
Data Protection Officer (Revised and Enhanced Policy Draft)	10/5/21
Leadership Team	20/7/21
Staff and Members	6/8/21 – 25/8/21

Policy Approval

This document requires the following approvals.

Approved by	Name	Date	Signature
National Park Authority	On File	TBC	On File

Contents

1. Purpose

The purpose of this Policy is to apply the principles of all relevant Data Protection legislation within Pembrokeshire Coast National Park Authority (the Authority).

The UK General Data Protection Regulation (GDPR) is implemented in the UK by the Data Protection Act 2018.

This Policy seeks to protect the rights and privacy of living individuals and to ensure that personal data (applying to all relevant information held on IT systems and all relevant paper-based data) is not processed without their knowledge and wherever relevant, is processed with their consent.

- To comply with the regulations, information about individuals must be collected and used fairly with a lawful basis, stored safely and securely and not disclosed unlawfully to any third party
- In addition to the regulatory requirements around the protection of personal data, this policy details the way in which other information should be managed
- The Authority strives to ensure it delivers fair outcomes for its customers and to its employees and volunteers. The Authority shall not knowingly, or intentionally breach any applicable laws or regulation relevant to the conduct of its business activities
- The Authority is committed to the highest standards of ethical conduct and integrity in its business activities and is dedicated to acting in an open and honest manner when dealing with customers, employees and volunteers
- This Policy should be read in conjunction with the wider suite of compliance policies that together provide a structure for employees and volunteers to work within ensuring they remain compliant with the Policy
- This Policy does not contain an exhaustive set of requirements. The Authority's employees, volunteers, Members and Contractors should always therefore comply with the spirit of this Policy, the overriding objective of which is to protect Personal Data held by the Authority
- Data Protection Guidance and detailed procedures for employees and volunteers can be accessed via Authority's intranet and departmental procedures are available from Team Leaders and heads of relevant service

areas. Best practice and specialist guidance is available on the Information Commissioner's Office Website.

2. Scope

This policy is applicable to all Authority employees, Members, volunteers, service users, contractors, consultants, collaborators and partners when collecting and processing personal data.

The Policy is owned by the Authority and accountability is delegated to the Chief Executive. The relevant governance and oversight activities are delegated to the Data Protection Officer.

3. Risk Appetite Background

The Authority has no appetite for regulatory breaches. The Authority has very low risk appetite for breaches of this policy and all related procedures.

4. Background

This policy aims to satisfy applicable data protection regulations in the UK which are:

- The UK General Data Protection Regulations (GDPR)
- The UK Data Protection Act 2018
- Privacy in Electronic Communications Regulations (PECR) 2003, updated in the e-privacy bill on 25th May 2018

Data Processing in the UK is regulated by the Information Commissioners Office (ICO), The Pembrokeshire Coast National Park Authority (the Authority) is registered with the ICO as a Data Controller, registration number Z6910336

This policy will be updated in accordance with any changes made to the aforementioned or related Regulations.

5. The Data Protection Principles

There are 7 key principles relating to the processing of personal data:

1. **Lawfulness, Fairness and Transparency –** Data should be processed lawfully, fairly and in a transparent manner in relation to the data subject

2. **Purpose Limitation –** Data should be collected for specified, explicit and legitimate purpose and not further processed in a manner that is incompatible with those purposes

3. **Data Minimisation -** Data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

4. **Accuracy –** Data should be accurate and where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate personal data, having regard to the purpose for which they are processed, are erased or rectified without delay

5. **Storage Limitation –** Data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed

6. **Integrity and confidentiality –** Data should be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organisational measures**.**

7. **Accountability –** This underpins all other principles. Organisations must take responsibility for the privacy and protection of all personal data that they process.

In respect of the 7 key principles for processing personal data; -

- The Authority is responsible for, and must be able to demonstrate compliance with, these conditions to the UK Information Commissioners Office (ICO). Failure to comply with applicable laws, rules and regulations could result in legal or regulatory sanctions, material financial loss or reputational loss to The Authority and lead to customer / member detriment.

- Any breach of this Policy may constitute a disciplinary, contractual, and criminal matter for individuals concerned and may cause serious damage to the reputation and standing of the Authority.

- The Authority may face criminal liability for unlawful actions taken by its employees, Members and volunteers.

- It is the responsibility of all employees, Members and volunteers to comply with the policy.

5.1 Lawfulness, fairness and transparency

5.1.1 Lawful basis for processing personal data

Processing of personal data is **only permitted** if one of the following applies; -

- It is done with the expressed consent of the data subject
- It is necessary for the provision of our service or the performance of a contract
- It is necessary for compliance with a legal action
- It is necessary to protect the vital interests of the data subject or another natural person

- It is necessary for the performance of a task carried out in the public interest
- It is necessary for the purpose of the legitimate interests

When using the lawful basis of legitimate interest, a 'Legitimate Interest Assessment' (LIA) should be completed to ensure that the interest is demonstrable.

5.1.2. Data Subject Consent Requirements

Where processing is based on consent; -

- The Authority must be able to demonstrate the data subject has consented to processing of personal data.
- If the data subject's consent is given in the context of a written declaration, which also concerns other matters, the request for consent must be presented in a manner that is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language.
- The data subject must have the right to withdraw their consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof.
- Any person whose details (including photographs) will be used to promote the Authority's work via publications, websites and social media will be asked to give consent. At the time the information is included or collected, all such individuals will be properly informed about the consequences of their data being disseminated outside of the UK.
- Photographs help staff to demonstrate the breadth of their work, and are used for publicity purposes when promoting the work of the Authority. Photographs and videos where people are identifiable should be carefully stored, with consent attached or cross referenced. Participants should be made aware of how images they appear in will be used by the Authority when providing consent. Staff should follow Authority guidance when taking photographs of crowds of people where consent may not be needed. Guidance is available on the Authority's intranet through the Taking Photos Protocol and Storage and Deletion Protocol for Photos.
- Special care should be taken in relation to taking, storing and using photographs of children, young people and vulnerable adults. Employees should follow the guidance provided on taking photographs and moving images for work purpose in the Authority's safeguarding statement.

5.1.3 Special Category Data

Special Categories of Data are more sensitive and thus warrant extra protection. The following are special categories of data as defined in the UK GDPR:

- ***racial*** or ***ethnic origin***
- ***political opinions***
- ***religious or philosophical beliefs***
- ***trade union membership***

- processing of ***genetic data***, ***biometric data*** for purposes of uniquely identifying a natural person
- data concerning ***health***
- data concerning a natural person's ***sex life or sexual orientation***

In order to process Special Category Data, in addition to establishing the lawful basis, one of the following 'conditions for processing' must apply:

(a) Explicit consent is obtained
(b) Processing is necessary for employment, social security and social protection (if authorised by law) purposes
(c) To protect the vital interests of the data subject or another natural person
(d) Undertaken by a not-for-profit body
(e) Made public by the data subject
(f) Necessary for legal claims or judicial acts
(g) For reasons of substantial public interest (with a basis in law)
(h) Health or social care (with a basis in law)
(i) Public health (with a basis in law)
(j) Archiving, research and statistics (with a basis in law)

Where **explicit consent** is relied upon, a record of the explicit consent must be retained.

5.1.4 Transparency

The Authority handles its obligations to inform data subjects via its Privacy Notice (sometimes referred to as a Privacy Policy). The Authority's privacy notice is available on the Authority's website.

Where personal data relating to a data subject is collected from the data subject, the Authority must at the time of collecting the personal data, provide the data subject with the following information; -

- The identity and contact details of who is collecting the data e.g., Pembrokeshire Coast National Park Authority (the Authority)
- The contact details for the Data Protection Officer (DPO) where appropriate
- The purposes of the processing as well as the legal basis for processing
- Where the processing is based on legitimate interests, what that interest is
- The third-party recipients or categories of recipients
- The period for which the personal data will be stored (or if this is not practically possible, state the criteria used to determine the period of retention)
- The existence of the right for the data subject to request from the Authority, access to, and rectification, or erasure of personal data, or restriction of processing concerning the data subject, or to object to processing as well as the right to portability (right to erasure is restricted where The Authority has a legitimate and lawful reason to retain data)

- Where processing of data is based on consent, the existence of the data subject's right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal
- The data subject's right to lodge a complaint with a supervisory authority (e.g., the ICO)
- Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter a contract, as well as whether the data subject is obliged to provide the personal data and to the possible consequences of failure to provide such data.
- The existence of any automated decision-making, including profiling, as well as the significance and the envisaged consequences
- When the data is used for a purpose other than that for which the personal data was collected, The Authority must also provide the data subject confirmation of this prior to that further processing.

This information shall be provided in writing or by other means, including where appropriate and practical, electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

5.2 Purpose Limitation

The Authority, its employees, Members and volunteers must only collect and process personal data for the purpose specified at the point of collection. When the data is used for a purpose other than for which it was collected, The Authority must provide the data subject with confirmation of this, prior to any further processing.

5.3 Purpose Minimisation

The Authority will collect, process, and create records containing personal data only to the extent that it is needed to fulfil operational needs, or to comply with any legal requirements. Such processing or creation of records will:

- Enable employees, Members and volunteers to carry out their work activities consistently, in full knowledge of the processes, decisions and actions that inform and drive the delivery of the Authority's complete services.
- Ensure the availability of credible and authoritative evidence to protect the rights of the Authority, its employees, its volunteers and customers.
- Demonstrate accountability by providing the evidence and information required for any internal or external audit
- Ensure all records are up to date and accurate
- Ensure only relevant data is captured, and personal data obtained is not excessive

5.4 Data Accuracy

Personal data processed by the Authority must be accurate and kept up to date. All reasonable steps must be taken to ensure that personal data that is inaccurate is erased or rectified without delay. Data subjects have the right to have any inaccurate data corrected at any time.

5.5 Storage limitations

5.5.1 Data Retention and Disposal

Information on the Authority's Retention Schedules are included in the Authority's Data Protection Record of Processing Activities and Data Retention Policy and Schedule. The Authority's Data Retention Schedules must be adhered to; -

- Retaining data for longer than is necessary constitutes a breach of regulations
- The data owners in the Authority determine and document the process to ensure data retention schedules are adhered to
- Data must be disposed of accordingly once it reaches the end of its retention period.
- The Authority's processes related to this Policy include how these practices are monitored
- Confidential and personal data must be securely and permanently deleted or disposed of once the retention requirements have been reached and must be disposed of in a way that protects the rights and privacy of data subjects
- All confidential and personal data is to be shredded and disposed of as 'confidential waste'. Hard drives and portable media must be disposed of securely as necessary

Redundant personal data will be destroyed using the Authority's procedure for disposal of confidential waste and deletion and erasure of electronic data. Clauses within contracts with data processors the Authority uses will include the requirement to delete or return all personal data to the controller as requested at the end of the contract.

5.6 Data Security

The Authority has appropriate security, technical and organisational measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Measures ensuring the level of security appropriate to risks of processing personal data include; -

- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- Maintain a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of Data Processing
- The pseudonymisation and encrypting of data when and where appropriate

The Authority has an ICT User Policy and Information and Data Security Policy that should be read in conjunction with this Policy.

5.6.1 Anonymisation Requirements

Anonymisation is the process of turning data into a form which does not identify individuals and where identification is likely to take place.

Personal data must be anonymised if it is to be used for a purpose other than which it was collected when consent was obtained (e.g., data analysis, system testing or training).

5.7 Accountability

The Authority takes accountability very seriously and as such ensures appropriate organisational and technical measures are implemented and reviewed continually.

- Ultimate accountability for Data Privacy sits with the Authority's Chief Executive who is personally responsible to the Authority
- All employees, Members and volunteers are individually responsible for ensuring they comply with the Authority's policies and procedures relating to data privacy
- Data Privacy Governance is delegated to the Authority's Data Protection Officer (DPO)
- The Authority's DPO must have suitable experience and expert knowledge of data protection law, as well as knowledge of the Authority's data protection needs and processing activities
- It is important to note a DPO is not personally liable for data protection compliance. The Authority remains responsible and accountable for compliance under data protection legislation.

5.7.1 Training

All employees, Members, volunteers and relevant contractors will undergo training outlining their responsibilities stated in this Policy. All employees, Members and volunteers and relevant contractors must undergo this training on induction into the Authority and subsequently, refresher training will be necessary on an ongoing basis (usually annually).

5.7.2 Documentation

The Authority maintains evidential documentation in demonstration of its compliance with the Regulations. This includes Records of Processing, Policies, Procedures and logs.

All documents are subject to a review period. All employees who process personal data must have access to the documented policies and procedures and be informed of what they are, the purpose they serve and must be trained on how to use them

(when/where applicable). Such documents should be made available, as applicable, via the Authority's internal intranet/ shared access folders.

6. Data Privacy by Design (and default)

The Data Protection Act 2018 (invoking the GDPR) requires the Authority to integrate data protection concerns into every aspect of its processing activities.

This approach is 'data protection by design and by default' which is a key element of the Data Protection Act 2018's risk-based approach and its focus on accountability, i.e., the Authority's ability to demonstrate how it complies with data privacy requirements.

6.1 Data Privacy Impact Assessments (DPIA)

DPIA's are a documented process helping organisations to identify and reduce data privacy risks of projects or process changes and should be used throughout the development and implementation of a project / change

- DPIA's enables the Authority to assess how a project or change may affect the privacy of individuals involved systematically
- A DPIA should be applied to new projects to allow greater scope for the project needs to be implemented and should also be used when planning changes to an existing system or 'business as usual (BAU) process
- A DPIA should ensure privacy risks are minimized, whilst allowing the project / change to meet its objectives
- Risks can be identified early in the project / change by assessing how data will be used (risks to data subjects such as potential for damage or distress)
- A DPIA should also assess corporate / commercial risks to the Authority, such as financial and reputational impacts of a breach arising from the project (higher risk projects that are likely to be more intrusive are likely to have a higher impact on privacy)

The DPIA process should not be overly complex or time consuming, but there are expectations that a certain level of rigor in proportion to the privacy risks arising from the project or change under review. The Authority has a documented process and a DPIA template which should be used and is available on the Authority's intranet.

7. Data Subject Rights

The Authority maintains appropriate procedures to facilitate data subjects exercising their rights. It will not refuse to act on requests from data subjects exercising their rights, unless the Authority can demonstrate they are unable to identify the data subject.

Data subjects have the right to:

- Be informed about the data processing activities

- Access the information the Authority holds about them (Data Subject Access Request Procedure)
- Have their details rectified if deemed inaccurate
- Have their details deleted if they are not required for lawful reasons
- Restrict the processing of their personal data
- Object to the processing of their data
- Request information processed by automated means is sent to them (or another nominated Data Controller) in a commonly used electronically readable format
- Certain provisions regarding the automated decision making and profiling

7.1 Subject Access Requests (SAR)

The Authority must ensure that Data subjects are able to exercise their SARs rights easily.

The Authority has (and maintains) an appropriate SAR Process in place that should be referred to in conjunction with this policy. All Data SAR received will be recorded for monitoring and reporting purposes on the appropriate log.

If requests are made electronically, the Authority will provide the information in a commonly used electronic format.

In most circumstances, the Authority will provide the personal information of the Data subject free of charge. However in limited circumstances the Authority may charge a reasonable fee to cover its administrative costs if it believes that the request is 'manifestly unfounded or excessive' or a Data subject asks for further copies of their information following a request. In these circumstances the one-month time limit does not begin until the Authority has received the fee. Any proposed decision to charge for a request should be reviewed and agreed with the DPO.

The Authority will provide individuals with a copy of the information held about them within one month of receiving a request.

On receiving such requests; -

- The Authority must check and require evidence to determine the identity of the individual and any further information required to clarify the specifics about the request being made
- Where a subject access request has a broad scope, the Authority may ask for more details from the data subject to locate the specific information that is of interest. Where large volumes of information are held, the Authority may seek to make the information available in ways other than providing a copy
- Requests from individuals to correct, rectify, block, or erase information they regard as incorrect, or to stop processing causing them damage or distress will be considered by the Authority on a case-by-case basis. The individual concerned will be fully informed of the resulting decision and the rationale behind the decision

- When a request for personal data is made by a third party and not on behalf of the data subject, the Authority shall consider the request under Freedom of Information, Environmental Information Regulations as well as Data Protection laws
- It shall consider whether releasing the personal data would breach any of the Data Protection principles and in particular whether any exemptions under Data Protection legislation apply so employees must first consult with the Data Protection Officer and Authority's Admin & Democratic Services Manager
- Personal information will not be shared with third parties unless specifically allowed for in law and justified in the specific situation

The Freedom of Information Publication Scheme deals with requests for information about third parties, and information will be withheld where disclosing it would breach any of the Data Protection principles. Where a requester does not state a specific reason for requesting the information then the Freedom of Information policy should be followed. A response to a Freedom of Information request must not take into account the reasons.

8. Data Sharing / Third Party Processing

8.1 Joint Controllers

Where two or more controllers jointly determine the purpose and means of processing data, it is referred to as being 'Joint Controllers'. Where this is the case, the Authority and the other Joint Controller shall (in a transparent manner) determine their respective responsibilities for compliance with the Data Protection Regulations, with regards to exercising the rights of data subjects and their respective duties to provide the information and gain consent.

Any data sharing between two Controllers must only be undertaken with the prior approval from the Authority's senior leaders and the Controllers and in conjunction with the DPO. A suitable Data Sharing Agreement must be in place between both parties. The Authority will follow best practice set out by the Wales Accord on Sharing Personal Information.

8.2 Using Data Processors

Where processing is to be carried out on behalf of the Authority by an appointed third party, only processors providing adequate guarantees to implement (or have) appropriate technical and organisational measures where processing meets the requirements of all Data Protection Regulations. A Data Processing Agreement (DPA) must be in place between the Controller and Processor setting out the details regarding the processing activities and security measures required.

Prior to engaging a third party in the processing activity, thorough due diligence is required to ensure third parties have the necessary organisational and technical measures in place to securely process data.

9. Data Breaches

The definition of a personal data breach means *'**a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'.***

A personal data breach may (if not addressed in an appropriate and timely manner) result in; -

- Physical, material or non-material damage to natural persons
- Loss of control over their personal data or limitation of their rights
- Discrimination
- Identity theft and/or fraud
- Financial loss
- Unauthorised reversal of pseudonymization
- Reputational damage
- Loss of confidentiality of personal data protected by professional secrecy
- Other significant economic or social disadvantages to the natural person concerned

The Authority's Data Breach Process should be read in conjunction with this policy.

As soon as The Authority becomes aware of a personal data breach, this should be considered very seriously and promptly.

All data breaches (however minor) should be reported via the process detailed within the Data Protection Breach Procedure document and must be reported without undue delay. Where feasible and appropriate (no later than 72 hours after having become aware of the breach), breaches should be escalated to the Information Commissioner's Office.

- The Authority will record all breaches, regardless of whether or not they need to be reported to the Information Commissioner's Office
- Links to records of these breaches will be added to the Data Protection Record of Processing Activities as they occur
- The Authority will document the facts relating to the breach, its effects and the remedial action taken.
- The Authority will investigate whether or not the breach was a result of human error or a systemic issue and see how a recurrence can be prevented – whether this is through better processes, further training, or other remedial action.

10. Complaint Handling Requirements

Processes and procedures are in place and maintained for handling data related complaints. The Chief Executive and the DPO must be notified of any upheld complaints relating to data protection. They must be kept informed of all correspondence relating to complaints. All data complaints should be processed in line with The Authority's Data Complaints Process.

- The first point of contact for data subjects should be the team or department which holds their data or is offering a service to them
- Matters should be resolved at a local level as quickly and effectively as possible with Officers and Managers to resolve complaints and run-on data requests
- Data Protection Complaints should be addressed to the Authority's Data Protection Officer: dpo@pembrokeshirecoast.org.uk
- If individuals are unhappy with how the Authority handles their information, they can also contact the Information Commissioner's Office to raise a concern via the following means:

Email: casework@ico.org.uk
Live chat function on ICO website: https://ico.org.uk/global/contact-us/live-chat/
Phone: 0303 123 1113. To phone them in Welsh call: 029 2067 8400.
Textphone Service: 01625 545860
Contact Address: Customer Contact Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

11. Monitoring

Ongoing monitoring to assess the adherence to, and effectiveness of this policy and related processes will be completed by Authority's Data Protection Officer, Leadership Team and Authority Members.

- The DPO, will review and monitor Data Privacy periodically via suitable reviews
- Monitoring should be conducted on a regular basis and no less than once annually
- Outputs from all monitoring activity will be reported to the Authority's Chief Executive and Leadership Team
- Internal Auditors may at times carry out data protection audits in order to monitor compliance with data protection law and this policy
- Reports on data protection and the operation of this policy will be made to Senior Management Team and the Authority's Audit and Corporate Services Review Committee

12. Data Privacy Governance

Roles and Responsibilities

First Line of Defence

All Employees, Members and Volunteers

- Are responsible for compliance with the Data Protection Policy and associated processes / procedures at all times
- Must report any potential, actual or perceived data breaches to their line manager who will review and escalate to the DPO when and where necessary to follow the data breach process (reporting potential / actual breaches)
- Acknowledge they have read and understood the Authority's data privacy related policies before being granted access to confidential or personal data relevant to their roles
- Ensure any required remediation for suspected or actual data breaches is resolved in a timely manner
- Complete all relevant Data Protection training and awareness, including the mandatory reading of all related policies

All Managers

- Are responsible for ensuring adherence to this policy and associated procedures and processes within their areas of the business
- Ensuring and monitoring that working practices within their areas of the business are compliant with all data protection regulations
- Must establish and maintain documented procedures to ensure anyone requesting confidential or personal data either in person, electronically or by telephone is appropriately authenticated before disclosing information
- Must establish and maintain documented procedures to ensure personal data relating to customers is kept accurate and up to date.

Second Line of Defence

Chief Executive and the DPO are responsible for ensuring; -

- The Authority's registrations with the ICO are maintained
- Ensuring that the Authority's policies and procedures are adequately defined and implemented to ensure compliance with all Data Protection Regulations
- They have oversight of, and confidence in, the first line activities and procedures to ensure compliance with all the requirements of this policy and associated processes / procedures
- They provide clarification and guidance with any aspect of compliance with all data protection regulations.

Members are responsible for; -

- Monitoring the Authority's performance on Data Protection compliance, including ongoing monitoring of risks identified on the risk register and responding to any concerns raised by the DPO or Information Commissioner's Office;
- Ensuring adequate resources are in place to fulfil the requirement of this policy and data protection law;
- Approving the appointment of a suitably qualified and competent DPO for the Authority.

14 Related Policies and Procedures

This policy should be interpreted and applied in relation to other related policies. A breach of any of these policies is likely also to be a breach of this policy. External policies are published on the Authority's website. Internal policies can be accessed from the Authority's intranet. These related policies include, but are not limited to:

- Freedom of Information Publication Scheme (External)
- ICT User Policy (External and Internal)
- Information and Data Security Policy (Internal)
- Safeguarding Statement (Internal)
- Social Media Protocol (Internal)
- Data Retention Policy and Schedule (External and Internal)

The following supporting documents and forms are available from the Authority's website:

- Freedom of Information Publication Scheme
- Privacy Notice
- Subject Access Request Form

The following supporting documents and forms are available from the Authority's intranet:

- Data Protection Record of Processing Activities
- Data Protection Impact Assessment Template
- Subject Access Request Procedure
- Data Protection Breach Procedure
- Data Breach Incident Form
- Procedure for the Disposal of Confidential Waste and deletion and erasure of electronic Waste
- Taking Photos Protocol
- Storage and Deletion Protocol for Photos.
- Legitimate Interest Assessment

15. Definitions

The Authority	Pembrokeshire Coast National Park Authority and any persons within the Authority who process Personal Data.
DP Legislation	All relevant data protection legislation, ICO codes of practice which apply to the Authority, including the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 and the Directive on Privacy and Electronic Communications (the ePrivacy Directive).
Data Subject	An individual who is the subject of any Personal Data.
DPIA	Data Privacy Impact Assessment
Explicit Consent	Where the Data Subject is asked to consent by a clearly defined 'Yes' or 'No' response.

Data Protection Officer (DPO)	The individual within the organisation who has oversight for data protection compliance.
GDPR	The UK General Data Protection Regulations.
ICO	The Information Commissioner's Office who are the UK regulator responsible for the oversight and enforcement of Data Protection legislation.
Personal Data	Data relating to a living individual.
Policy	The Data Protection Policy.
Principles	The eight Data Protection Principles outlined in the DP Legislation.

16. Reference

Wales Accord on Sharing Personal Information	http://www.waspi.org/home
Information Commissioner's Office Guidance	https://ico.org.uk/
Pembrokeshire Coast National Park Authority website	www.pembrokeshirecoast.wales
Pembrokeshire Coast National Park Authority's Overarching Privacy Notice	https://www.pembrokeshirecoast.wales/privacy/
Authority's Data Subject Access Request Form	*[Updated link to be added following review of form]*

17. The Authority's Data Protection Officer Contact Details

Contact Number	01646 624800
Contact Email	dpo@pembrokeshirecoast.org.uk
Correspondence Address	National Park Offices, Llanion Park, Pembroke Dock, Pembrokeshire, SA72 6DY

18. Version History

Version	Effective Date	Summary of Changes
2	4 September 2019	• Approved Policy
2	12 April 2021	• Name of Data Protection Officer amended

3	(Insert date once policy approved)	• Revised and enhanced policy draft following review by Authority's DPO