Pembrokeshire Coast National Park Authority

POL_006 Data Protection Policy

Parc Cenedlaethol Arfordir Penfro
Pembrokeshire Coast National Park

External and Internal Policy

Review

Version	Active Policy	Document Owner	Review Date Trigger
2	4 September 2019	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
Staff and Staff Reps	9 August 2019

Approvals

This document requires the following approvals.

Approved by	Name	Date	Signature
Leadership Team	On File	25 June 2019	On File
National Park Authority	On File	4 September 2019	On File

Contents

1. Policy Statement

Pembrokeshire Coast National Park Authority (the Authority) is fully committed to compliance with the requirements of the Data Protection Act 2018 and other relevant Data Protection laws.

The Authority will therefore aim to ensure that all employees, Members, volunteers, contractors, consultants or partners of the Authority who have access to any personal data held on behalf of the Authority, are fully aware of and abide by their duties and responsibilities under the relevant regulations and laws.

The Authority's Data Protection Officer's Contact Details

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

2. Purpose and Scope

2.1 The Authority needs to collect and use certain types of information about people it deals with in order to perform its functions. This includes information on current, past and prospective employees, Members, volunteers, suppliers, clients, customers, service users, supporters and others with whom it communicates.

2.2 The Authority is required by law to collect and use certain types of information to fulfil its statutory responsibilities and also to comply with the legal requirements set out by Government.

2.3 It is essential that the Authority treats personal information lawfully and correctly. This is critical to successful operations, fulfilling our statutory responsibilities and maintaining public confidence in the Authority. As a data controller we set out the legal basis for the processing of the data we collect and use in the Authority's Data Register.

2.4 The purpose of this policy is to explain how the Authority will ensure compliance with the relevant data protection regulations and laws. It includes organisational measures and individual responsibilities which aim to ensure that the Authority complies with the Data Protection principles and respects the rights of individuals.

2.5 Detailed procedures and guidance do not form part of this overarching policy document. Data Protection Guidance for staff can be accessed via Parcnet and departmental procedures are available from Team Leaders and heads of relevant service areas.

3. Legal Context

3.1 Data Protection is governed by legislation, including:

a) The Data Protection Act 2018;
b) The General Data Protection Regulations;
c) Human Rights Act 1998;
d) Freedom of Information Act 2000;
e) Environmental Information Regulations 2004;
f) Computer Misuse Act 1990;
g) Privacy and Electronic Communications Regulations 2003;
h) Equality Act 2010;
i) Common law duty of confidentiality: Employer's common law duty to employees to maintain a relationship of mutual trust and confidence.

4. What is Personal Information?

There are two key types of 'personal information' in the United Kingdom and they cover different categories of information. They are:

Personal Data:

4.1 This can be anything that allows a living person to be directly or indirectly identified.

4.2 This can include: name, address, email address, home telephone or personal mobile numbers, employment information, bank details, national insurance numbers, file notes linked to an individual, images including CCTV footage, online identifiers and IP addresses. This is not an exclusive list. This data may be held in hard copy or electronically.

4.3 It includes automated personal data and can also encompass pseudonymised data if a person can be identified from it.

Sensitive Personal Data:

4.4 The GDPR and Data Protection Act 2018 identify 'special categories' of sensitive personal information that need more protection.

4.5 This includes information on a person's race, ethnic origins, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life; or sexual orientation.

Equality Monitoring Data

4.6 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.

5. Data Subjects, Controllers and Processors

5.1 A **Data Subject** is an individual who is the subject of the data. For the Authority data subjects may include employees, job applicants, Members, volunteers, suppliers, contractors, customers, event attendees, clients, service users, website visitors, supporters and others whom we communicate or liaise with.

5.2 A **Data Controller** is an organisation, or person that determines the purposes for which and the manner in which any personal data is to be processed. As a data controller we set out the legal basis for the processing of the data we collect and use in the Authority's Data Register.

5.3 A **Data processor** is any organisation or person (other than an employee of the data controller) who processes data on behalf of the data controller. Where the Authority's databases are hosted by other companies the Authority remains the data controller and the host company acts as the data processor.

6. Data Protection Principles

6.1 The Data Protection principles set out the main responsibilities that the Authority and organisations must legally comply with.

6.2 The data protection principles require that *under* Article 5 of the GDPR personal data shall be:

a) Processed lawfully, fairly and in a transparent manner in relation to individuals;

b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; 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 subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) 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.

6.3 Data Controllers under Article 5(2) of the GDPR are also responsible for, and must be able to demonstrate, compliance with the principles.

6.4 In order to meet the requirements of the principles, the Authority will:

a) Observe fully the conditions regarding the fair collection and use of personal data;
b) Meet its obligations to specify the purposes for which personal data is used, listing them in the Authority's data register;
c) Collect and process appropriate personal data only to the extent that it is needed to fulfil operational or any legal requirements;
d) Ensure the quality of personal data used;
e) Apply strict checks to determine the length of time personal data is held;
f) Ensure that the rights of individuals about whom the personal data is held, can be fully exercised under relevant laws;
g) Take the appropriate technical and organisational security measures to safeguard personal data;
h) Ensure that personal data is not transferred abroad without suitable safeguards;
i) Have appropriate accountability mechanisms in place including appointing a Data Protection Officer, carrying out data protection impact assessments and use of relevant clauses in contracts with data processors.

7. Lawful Basis of Processing

7.1 The Authority will collect and process personal data only to the extent that it is necessary to fulfil operational needs or to comply with any legal requirements. The purpose for processing data and legal bases for the processing of the data are set out in the Authority's Data Register.

7.2 The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply when the Authority processes personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

7.3 Where the Authority collects and processes sensitive personal data it will ensure that at least one of the conditions for processing special category data applies and the condition will be listed in the Authority's data register.

7.4 The conditions for processing special category data under Article 9(2) of the GDPR are:

(a) The data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) Processing relates to personal data which are manifestly made public by the data subject;

(f) Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) Processing is necessary for reasons of public interest in the area of public health, such as 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, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

8. Consent

8.1 Where individual consent is needed to process personal data the consent must be free and informed and may be changed at any time.

8.2 The GDPR and Data Protection Act 2018 set a high standard for consent. An indication of consent must be unambiguous and involve a clear affirmative action (an opt-in). Pre-ticked opt-in boxes are not permitted. Individual ('granular') consent options for distinct processing operations are required. Consent should be separate from other terms and conditions and should not generally be a precondition of signing up to a service.

8.3 The GDPR and Data Protection Act 2018 gives a specific right to withdraw consent. The Authority will tell people about their right to withdraw, and offer them easy ways to withdraw consent at any time.

8.4 The Authority will keep records of where consent has been given.

8.5 Relying on inappropriate or invalid consent could harm the Authority's reputation – and may leave the Authority open to large fines. The Authority will only use consent as appropriate lawful basis if it can offer people real choice and control over how their data is used, and wants to build their trust and engagement. If the Authority cannot offer a genuine choice, consent is not appropriate. For example cases where we would still process the personal data without consent, in these cases asking for consent is misleading and inherently unfair. If the Authority make consent a precondition of a service, it is unlikely to be the most appropriate lawful basis.

8.6 ICO guidance notes that "Public authorities, employers and other organisations in a position of power over individuals should avoid relying on consent unless they are confident they can demonstrate it is freely given." This is particularly relevant for areas relating specifically to the Authority's public functions.

8.7 When sensitive data is collected, the Authority will obtain the individual's explicit consent for this processing unless another clear legal basis for processing sensitive personal data has been identified.

8.8 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 worldwide.

8.9 When personal data is to be used for a new purpose, if necessary a new consent will be sought.

9. Consent and Images

9.1 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 moving images 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.

9.2 Special care should be taken in relation to taking, storing and using photographs of children, young people and vulnerable adults. Staff should refer to and follow guidance provided on taking photographs and moving images for work purpose in the Authority's safeguarding statement.

9.3 Staff should follow Authority guidance when taking photographs of crowds of people where consent may not be needed.

10. Rights of the Individual

10.1 The GDPR and Data Protection Act 2018 provides the following rights for Data Subjects:

1. The right to be informed;
2. The right of access;
3. The right to rectification;
4. The right to erasure;
5. The right to restrict processing;
6. The right to data portability;
7. The right to object;
8. Rights in relation to automated decision making and profiling.

10.2 The legal basis of processing influences which rights are available to the individual. The Authority's data register outlines what rights are available to the individual in relation to information processed by the Authority in terms of its corresponding lawful basis for processing.

11. Privacy Information – Fair Processing/Privacy Notices

11.1 The Authority will, as far as is practicable, ensure that all individuals whose details are processed are aware of the way in which that information will be held, used (purpose of processing), retention period for that data and who it will be shared with. Individuals will, where possible, be informed of the likely recipients of the information – whether the recipients are internal or external to the Authority.

11.2 This information will be provided when personal data is first collected, whether written or verbal.

11.3 The Authority's overarching privacy notice will be made available on the Authority's website [4].

11.4 Information the Authority provides to people in fair processing/privacy notices will be concise, transparent, intelligible, easily accessible, and use clear and plain language. These notices will be tailored for the audience they are being provided to. When personal data is to be used for a new purpose then this information will be provided to the data subject again and if necessary a new consent will be sought.

11.5 People can ask for more details about how their personal data is being used at any time and, if unhappy about how their data is used, may make a complaint.

11.6 The Authority will regularly review, and where necessary, update privacy information and notices. This process will also be aligned to changes needed following any review or update of the data register.

12. Data Accuracy and Rectification

12.1 The Authority will ensure, as far as is practicable, that the information it holds is accurate and up-to-date.

12.2 If personal data is found to be inaccurate, this will be remedied as soon as possible.

12.3 Personal information, such as contact details, may be shared within the Authority where it is necessary to keep records accurate and up-to-date, and in order to provide individuals with a better service.

12.4 Records may include professional opinions about individuals but employees will not record any personal opinions about individuals.

13. Subject Access Requests

13.1 Under the GDPR and Data Protection Act 2018, individuals have the right to obtain:

a) Confirmation that their data is being processed;
b) Access to their personal data; and
c) Other supplementary information – this largely corresponds to the information that should be provided in a privacy/ fair processing notice.

13.2 The reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing.

13.3 A person who wishes to exercise this right can make a written or verbal request to the Authority.

13.4 Data Subjects can also fill out the Authority's Subject Access Request form [5]. This form is available from the Authority's Administration & Democratic Services Manager and the Authority's website. If a person requires assistance in completing the form, needs the form in an alternative format they should contact the Admin & Democratic Services Manager.

13.5 We will verify the identity of the person making the request, using 'reasonable means'.

13.6 If the request is made electronically, we will provide the information in a commonly used electronic format.

13.7 In line with regulations a copy of the information will be provided free of charge as required under GDPR. However, the Authority will charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive. The Authority may charge a reasonable fee to comply with requests for further copies of the same information. The fee will be based on the administrative cost of providing the information.

13.8 Information will be provided within one month of receipt of the request. Where a request is complex or numerous the Authority will seek to extend the period of compliance by a further two months with the consent of the Information Commissioner's Office. In these cases the Authority will inform the individual within one month of the receipt of the request and explain why the extension is necessary. If the request is made electronically, the authority will provide the information in a commonly used electronic format.

13.9 If requests are manifestly unfounded or excessive, in particular because they are repetitive, the Authority may refuse to respond. If the Authority refuses to respond to a request we will explain why to the individual, informing them of their right to complain to the Information Commissioner's Office and to a judicial remedy within one month.

13.10 Where the Authority processes a large quantity of information about an individual, the GDPR permits us to ask the individual to specify the information the request relates to (Recital 63). The legislation does not include an exemption for requests that relate to large amounts of data, but the Authority may be able to consider whether the request is manifestly unfounded or excessive.

14. Third Party Access to Information

14.1 Where a request for personal data is made by a third party on behalf of the data subject, it shall be treated as a subject access request. Evidence is required that the third party is entitled to act in this way, such as a written statement from the data subject or an enduring power of attorney. Appropriate professionals may need to be consulted before a decision to release the personal data is made.

14.2 Occasionally third party information may form part of the data extracted in response to a subject access request. In deciding whether to release this information, the Authority will consider the following:

a) Any duty of confidentiality owed to the third party;
b) Attempts to get consent from the third party;
c) Any express refusal of consent from the third party;
d) The third party's expectations with respect to that data.

14.3 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 as well as GDPR and 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. Employees should 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.

14.4 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 behind the request.

14.5 When there is a specific reason for requesting the information, an exemption under Data Protection Legislation may apply. Examples are where information is required for the prevention or detection of crime, apprehension or prosecution of offenders or assessment or collection of tax. If an appropriate exemption under Data Protection legislation does apply so that the Data Protection principles will not be breached, the Authority will usually comply with the request.

14.6 Where the Authority is not convinced that the third party has entitlement to the personal data, or that any exemptions under Data Protection legislation apply, and that releasing information would breach the Data Protection principles, the personal data will be withheld and only released on presentation of a Court Order.

15. Sharing Information

15.1 Information sharing occurs when an organisation shares information about a data subject for the better provision of a service or where it is in the best interests of that data subject.

15.2 The Authority promotes information sharing where it is in the best interests of the data subject. However, personal sensitive data (special category data) will not be shared unless it is in connection with the primary purpose for which the information was collected, or the data subject has explicitly given their permission for the information to be shared for this purpose, or another legal provision relating to the processing of special category data allows for the sharing of such information.

15.3 The Authority will ensure that supporting processes and documentation are made available to the Authority's staff so that they understand how to share information safely and lawfully. Where an employee acting in good faith has shared information in accordance with these supporting processes and documentation, they shall not normally be subject to disciplinary action.

15.4 Sharing large sets of information or recurrent regular sharing shall be carried out under written agreement to ensure the continued compliance with the data protection laws and that additional safeguards can be considered and put in place.

15.5 The Authority may enter into data sharing arrangements with other public bodies. Where this occurs the Authority will do so in accordance with the Data Protection principles and formal data sharing arrangements, following best practice set out by the Wales Accord on Sharing Personal Information [1].

16. Retention and Erasure

16.1 The Authority's use of personal data will comply with its Retention Schedule covering the different types of records held by the Authority. Information on Retention Schedules are included in the Authority's data register.

16.2 Information will only be held for as long as is necessary after which the details will normally be deleted or disposed of. Where details of individuals are stored for long-term archive or historical reasons, and where it is necessary to retain the personal detail within the records, it will be done within the requirements of the legislation.

16.3 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.

16.4 The Authority will ensure relevant processes are in place to enable the erasure of data where a data subject wishes to exercise their right to have their personal data erased and where they are entitled for this erasure to happen. The Authority will follow Information Commissioner's guidance on the Right to Erasure where requests are made.

17. Information Security

17.1 The Authority will implement appropriate technical and organisational security measures so that unauthorised staff and other individuals are prevented from gaining access to personal information.

17.2 The Authority recognises that poor information security leaves the Authority systems and services at risk and may cause real harm and distress to individuals. Harm that can be caused by loss or abuse of personal data include:

a) Identity fraud;
b) Fake credit card transactions;
c) Targeting of individuals by fraudsters, potentially made more convincing by compromised personal data;
d) Witnesses and planning objectors put at risk of physical harm or intimidation;
e) Exposure of the addresses of vulnerable people and those at risk of domestic violence or harassment;
f) Fake applications for tax credits;
g) Mortgage fraud;
h) Discrimination;
i) Personal embarrassment and impact on well-being of individual affected.

17.3 An employee must only access personal data they need to use as part of their job. Inappropriate or unauthorised access may result in disciplinary action, including dismissal and criminal prosecution.

17.4 The Authority has an ICT User Policy which applies to electronic systems containing personal data. The Authority's Information and Data Security Policy is managed by the Head of ICT. All ICT security incidents should be reported to the ICT Helpdesk.

17.5 Personal data held on computers and computer systems will be installed with user-profile type password controls, encryption where possible and where necessary audit and access trails to establish that each user is fully authorised.

17.6 Manual files and other records or documents containing personal/sensitive data will be kept in a secure environment and accessed on a need-to-know basis only.

17.7 All managers, team leaders and staff within the Authority departments and Authority Members will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure.

17.8 Managers and Team leaders should ensure relevant procedures and protocols are in place for their department or team and that staff within their team and department are aware and follow these procedures.

17.9 Employees who process personal data out of the office (e.g. on site, on client premises, at home) can only do this with the express consent of their manager. Staff should follow relevant procedures to keep this information safe.

17.10 Access to personal data outside of the Authority should not be attempted using unsecured access systems (this includes via mobile networks outside of UK unless the network has been checked in advance to be compliant under data protection law).

17.11 System testing will only be carried out using personal data where sufficient safeguards are in place and will not be undertaken on live databases accessing live personal sensitive data.

17.12 Personal data will not be transferred outside the European Economic Area without the approval of the Data Protection Officer.

17.13 Information Security will be considered as part of data protection impact assessments. Security measures for different sets of data will be listed within the Authority's data register.

17.14 Appropriate procedures will be in place for the safe disposal of paper waste and electronic data containing personal information.

17.15 All data breaches (however minor) should be reported via the process detailed within the Staff Data Protection Guidance.

17.16 Security arrangements will be reviewed regularly, any reported breaches or potential weaknesses will be investigated and, where necessary, further or alternative measures will be introduced to secure the data.

18. Accountability and Governance

18.1 The Authority will put in place relevant and proportionate processes to promote accountability and governance in its collection, processing and use of personal information. These measures aim to minimise the risk of breaches, encourage continued improvement in data management practices and uphold the protection of personal data.

19. Data Protection Officer

19.1 The Authority has a legislative duty as a Public authority to appoint a Data Protection Officer.

19.2 The Authority's appointed Data Protection Officer will:

a) Inform and advise the Authority and its employees about their obligations to comply with data protection legislation;
b) Monitor compliance with the data protection legislation, and with the Authority's policies, including managing internal data protection activities, raising awareness of data protection issues, training staff and conducting internal audits;
c) Advise on, and monitor, data protection impact assessments;
d) Cooperate with the supervisory authority;
e) Be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.). Their work contact details will be readily available to the Authority's employees, to the Information Commissioner's Office, and people whose personal data the Authority processes;
f) Have experience and expert knowledge of data protection law as well as the Authority's data protection needs and processing activity;
g) Be given the authority to act independently on matters concerning data protection compliance within the Authority;
h) Report to Members, the Chief Executive and Senior Management Team;
i) Report annually to the Audit and Corporate Services Committee on Authority's performance on Data Protection compliance;
j) Provide risk based advice to the organisation. Where an increased risk is identified due for example to a change in the nature of data collected or how data is processed by the Authority, The Data Protection Officer will ensure this is reflected in the Authority's risk register;
k) Submit the registration notification and any amendments (if necessary) to the Information Commissioner.

19.3 The Authority will ensure that:

a) The Data Protection Officer is involved closely and in a timely manner, in all data protection matters;
b) The Data Protection Officer reports to Members, Chief Executive or Senior Management Team;
c) The Data Protection Officer operates independently and is not dismissed or penalised for performing their tasks;
d) Provide adequate resources (sufficient time, financial, infrastructure, and, where appropriate, staff) to enable the Data Protection Officer to meet their data protection legislation obligations, and to maintain their expert level of knowledge;
e) Give the Data Protection Officer appropriate access to personal data and processing activities;

f) Give the Data Protection Officer appropriate access to other services within the Authority so that they can receive essential support, input or information;
g) Seek the advice of the Data Protection Officer when carrying out a Data Protection Impact Assessments;
h) Details of the Data Protection Officer are recoded as part of our records of processing activities;
i) If it decides not to follow the advice given by its appointed Data Protection Officer, it will document its reasons to help demonstrate accountability.

19.4 The Authority's Data Protection Officer can be an existing employee or externally appointed. Where a Data Protection Officer is an existing employee the Authority will ensure that their current role doesn't result in a conflict of interest with their primary tasks as a Data Protection Officer and the Authority will implement any mitigating actions to this effect. The Data Protection Officer will not hold a position within the Authority that leads them to determine the purposes and the means of the processing of personal data. The Data Protection Officer will not be expected to manage competing objectives that could result in data protection taking a secondary role to business interests.

19.5 The Data Protection Officer isn't personally liable for data protection compliance. As the controller or processor the Authority remains responsible for compliance under data protection legislation.

20. Data Protection Impact Assessments

20.1 A data protection impact assessment (DPIA) is a process the Authority will use to help identify and minimise the data protection risks of a project.

20.2 The Authority must do a Data Protection Impact Assessment for the following listed types of processing or any other processing that is likely to result in a high risk to individual's interests:

a) Use systematic and extensive profiling with significant effects;
b) Process special category or criminal offence data on a large scale; or
c) Systematically monitor publicly accessible places on a large scale;
d) Use new technologies;
e) Use profiling or special category data to decide on access to services;
f) Profile individuals on a large scale;
g) Process biometric or genetic data;
h) Match data or combine datasets from different sources;
i) Collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');
j) Track individuals' location or behaviour;
k) Profile children or target services at them; or
l) Process data that might endanger the individual's physical health or safety
in the event of a security breach.

20.3 Even if there is no specific indication of likely high risk, it is good practice to do a Data Protection Impact Assessment for any major new Authority project involving the use of personal data.

20.4 The Data Protection Impact Assessment will:

a) Describe the nature, scope, context and purposes of the processing;
b) Assess necessity, proportionality and compliance measures;
c) Identify and assess risks to individuals; and
d) Identify any additional measures to mitigate those risks.

20.5 To assess the level of risk the Authority will consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

20.6 The Authority's staff will consult with the Authority's Data Protection Officer and, where appropriate, individuals and relevant experts. Staff should consult with relevant external processors when completing an assessment.

20.7 If the Authority identifies a high risk and we cannot mitigate that risk, we will consult the Information Commissioner's Office before starting the processing.

20.8 The Information Commissioner's office will give written advice within eight weeks, or 14 weeks in complex cases. In appropriate cases they may issue a formal warning not to process the data, or ban the processing altogether.

20.9 A link to completed Data Protection Impact Assessments will be listed against relevant items on the data protection register.

21. Documentation – Data Register

21.1 The Authority is required to maintain a record of the Authority's processing activities; this is done through Authority's data register.

21.2 The Authority as required under Article 30 of the GDPR will document the following information in its Data register:

a) The Authority's name and contact details and the name and contact details of the Authority's Data Protection Officer;
b) The purpose of the Authority's processing;
c) A description of the categories of individuals and categories of personal data;
d) The categories of recipients of personal data;
e) Details of any transfers to third countries including documenting the transfer mechanism safeguards in place;
f) Retention schedules;
g) A description of your technical and organisational security measures.

21.3 The register also documents or links to other aspects of the Authority's compliance with GDPR and other data protection laws and is based on the Information Commissioner's template register for Data controllers. Other areas covered includes:

a) The lawful basis for the processing;
b) The legitimate interests or Public Task for the processing of individuals' rights;
c) The existence of automated decision-making, including profiling;
d) The source of the personal data;
e) Records of consent;
f) Controller-processor contracts;
g) The location of personal data;
h) Data Protection Impact Assessment reports;
i) Records of personal data breaches.

22. Contracts

22.1 Whenever the Authority uses a processor (a third party who processes personal data on behalf of the controller) it will have a written contract in place, this is so that both parties understand their responsibilities and liabilities.

22.2 Contracts will include as required by the Authority:

a) The subject matter and duration of the processing;
b) The nature and purpose of the processing;
c) The type of personal data and categories of data subject;
d) The obligations and rights of the controller.

22.3 Contracts as required by GDPR will also include as a minimum the following terms, requiring the process to:

a) Only act on the written instructions of the controller;
b) Ensure that people processing the data are subject to a duty of confidence;
c) Take appropriate measures to ensure the security of processing;
d) Only engage sub-processors with the prior consent of the controller and under a written contract;
e) Assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
f) Assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
g) Delete or return all personal data to the controller as requested at the end of the contract; and

h) Submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

22.4 The Authority is liable for its compliance with the GDPR and must only appoint processors who can provide 'sufficient guarantees' that the requirements of the GDPR will be met and the rights of data subjects protected.

22.5 Under GDPR processors must only act on the documented instructions of a controller. Processors do have some direct responsibilities under the GDPR and may be subject to fines or other sanctions if they don't comply.

23. Concern or Complaint about how the Authority Uses Data

23.1 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.

23.2 Data Protection Complaints should be addressed to the Authority's Data Protection Officer: Sarah Burns (dpo@pembrokeshirecoast.org.uk)

23.3 If individuals are not happy about how the Authority has handled their information they can 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

24. Data Breaches and Reporting

24.1 A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. It is important to remember that a breach is more than just about losing personal data.

24.2 Personal data breaches can include:

a) Access by an unauthorised employee or third party;
b) Unauthorised disclosure of personal data, including sending personal data to an incorrect recipient;
c) Deliberate or accidental action (or inaction) by a controller or processor;
d) computing devices or paper documents containing personal data being lost or stolen;
e) Alteration of personal data without permission; and
f) Loss of availability of personal data, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

24.3 When a security incident takes place, the Authority will act quickly to establish whether a personal data breach has occurred and, if so, promptly take steps to address it. As part of this assessment the Authority will establish the likelihood and severity of the resulting risk to people's rights and freedoms and whether the Information Commissioner's Office and individuals affected need to be notified.

24.4 The Authority has a legal duty to report certain types of personal data breach to the Information Commissioner's Office. This must done within 72 hours of becoming aware of the breach, where feasible. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the Authority must also inform those individuals without undue delay. If the Authority isn't able to provide full details within 72 hours, we will explain the delay to the ICO and tell them when we expect to submit more information. Article 34(4) of GDPR allows the Authority to provide the required information in phases, as long as this is done without undue further delay. Failing to notify the Information Commissioner's Office of a data breach when required to do so could result in a fine up to 10 million euros or 2 per cent of an organisations global turnover. The fine can be combined with the ICO's other corrective powers under Article 58.

24.5 The Authority will allocate responsibility for managing breaches to a dedicated person or team. When reporting a breach, the Authority will provide the following information as set out in GDPR:

a) A description of the nature of the personal data breach including, where possible:
   - The categories and approximate number of individuals concerned; and
   - The categories and approximate number of personal data records concerned;

b) The name and contact details of the Authority's Data Protection Officer;
c) A description of the likely consequences of the personal data breach; and
d) A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

24.6 When the Authority notifies an individual of a breach it will provide information in clear and plain language on the nature of the personal data breach and, at least:

a) The name and contact details of the Authority's Data Protection Officer;
b) A description of the likely consequences of the personal data breach; and
c) A description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

24.7 The Authority will ensure that staff know how to recognise a personal data breach. Staff will be encouraged to report all breaches (however minor) following the process detailed within the Staff Data Protection Guidance.

24.8 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 register 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 corrective steps.

24.9 Where relevant the Authority may also consider notifying third parties such as the police, insurers, professional bodies, or bank or credit card companies who can help reduce the risk of financial loss to individuals.

25. Information Commissioner's Office - Notification

25.1 The Authority is required to register with the Information Commissioner's Office; it is registered under number Z6910336. The Authority will ensure that this notification is an accurate description of processing carried out by the Authority.

25.2 The Data Protection Officer is responsible for submitting this notification to the Information Commissioner. When the Authority plans to carry out new processing not covered by this notification, the officer responsible will inform the Data Protection Officer in good time to amend the notification (if necessary) within 28 days of processing beginning.

25.3 Processing of personal data by Members is covered by the Authority's main corporate notification in respect only of information held by the Authority.

25.4 Failure to notify or maintaining an incomplete or inaccurate notification is a criminal offence.

26. Responsibility for Implementation of the Policy

26.1 The Authority has responsibility for ensuring that:

a) Everyone managing and/or handling personal information understands that they are contractually responsible for following good data protection practice, and that they may commit criminal offences if they deliberately try to access or disclose personal data without authority;
b) Everyone managing and/or handling personal information is appropriately trained to do so;
c) Everyone managing and/or handling personal information is appropriately supervised and are aware of specific procedures relevant for their team or job roles;
d) Anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, is given advice as necessary;
e) Queries about handling personal information are promptly and courteously dealt with;
f) Methods of handling personal information are regularly assessed and evaluated;
g) Employees are aware of the action required in the event of a Data Breach;
h) Data Register and Privacy Information is kept up to date;
i) Data Impact Assessments are completed where required;
j) Guidance for staff is updated and regular awareness raising activities are carried out.

26.2 Members have responsibility for ensuring that they:

a) Monitor the Authority's performance in relation to Data Protection Compliance, including ongoing monitoring of risks identified on the risk register and responding to any concerns raised by the Data Protection Officer or Information Commissioner's Office;
b) Ensure adequate resources are in place to fulfil the requirement of this policy and data protection law;
c) Appoint a Data Protection Officer for the Authority;
d) Adhere to this policy and other relevant policies when handling personal data within their role as a Member of the Authority;
e) Report any data breaches (however minor) following the procedure set out in the Staff Data Protection Guidance;
f) They report any concerns and seek advice from the Data Protection Officer.

26.3 Chief Executive and Senior Management Team have responsibility for ensuring that they:

a) Provide leadership on data compliance and promote the delivery of the data protection principles across the Authority;
b) Respond to any concerns raised by the Data Protection Officer and comply with section 19 of the policy;
c) Respond to any enforcement action brought against them by the Information Commissioner's Office;
d) Ensure adequate resources are in place to enable accountability and implementation measures to be delivered;
e) Ensure the risk register, data register, relevant policies and privacy notices across organisation are in place and amended as needed;
f) Ensure decisions made about projects and proposals are informed by outcomes from data impact assessments;
g) Ensure that they adhere to this policy when handling personal data within their role;
h) Ensure this and other related policies are being implemented effectively.

26.4 Leadership Team have responsibility for ensuring:

a) Outcomes of data protection impact assessments are considered when making decisions on new projects and proposals;
b) They address and develop as a group organisational information governance solutions that promote best practice and help minimise the risk of data protection breaches;
c) Information Governance Mechanisms relating to document management on the shared drive are being followed and identify actions to address issues that arise.

26.5 The Data Protection Officer has responsibility for ensuring that:

a) They fulfil their duties as set out in section 19 of this policy.

27.6 IT Manager has responsibility for ensuring that

a) They fulfil IT security duties as set out in ICT User Policy and this policy, being responsive to changes in security best practice.

26.7 Team Leaders have responsibility for ensuring that:

a) Relevant data protection procedures are in place and being followed by staff within their team;
b) That new staff at induction are provided with guidance and relevant training on Authority and team procedures on data protection relevant to their role;

c) That refresher training and guidance is given to team members if new data is captured and/or ways of processing or knowledge gaps are identified;
d) They notify the Data Protection Officer of changes and amendments needed to the Data register;
e) Ensuring relevant privacy notices and consent information and records are in place where needed for their department;
f) They carry out Data Protection Impact Assessments as required or assist staff within their team with completing an assessment;
g) They monitor record keeping and storage within team to ensure they are following the Authority record management policy;
h) Employee information is processed in accordance with this policy, the record management policy and guidance issued by personnel;
i) Adhere to this policy and other relevant policies when handling personal data;
j) Report any data breaches (however minor) following the procedure set out in the Staff Data Protection Guidance;
k) They report any concerns to and seek advice from the Data Protection Officer.

26.8 Individual Staff have responsibility for ensuring that they:

a) Follow the Staff Data Protection Guidance and relevant data protection procedures for the Authority or specific to their team;
b) Attend training and awareness sessions arranged and notify their line Manager if they require additional training or guidance;
c) Notify their team leader or the Data Protection Officer directly of changes and amendments needed to the data register;
d) Complete Data Protection Impact Assessments as required with assistance of their team leader and the Data Protection Officer;
e) Follow Authority record retention schedule;
f) Adhere to this policy and other relevant policies when handling personal data;
g) Report any concerns to and seek advice from the Data Protection Officer.

26.9 Volunteers have responsibility for ensuring that they:

a) Adhere to this policy and Staff Data Protection guidance when handling personal data;
b) Follow the Staff Data Protection Guidance and relevant data protection procedures for the team they are volunteering with if they are handling personal data;
c) Report any data breaches (however minor) following the procedure set out in the Staff Data Protection Guidance;
d) Report any concerns to and seek advice from the Data Protection Officer.

26.10 Partners and contractors have responsibility for ensuring that:

a) They and all of their staff who have access to personal data held or processed for or on behalf of the Authority, are aware of this policy and are fully trained in and are aware of their duties and responsibilities under data protection law.
b) Any observed or suspected security incidents or security concerns should be reported to the Authority's Data Protection Officer.
c) They allow data protection audits by the Authority of data held on its behalf if requested in line with contractual arrangements.

27. Other Related Policies and Supporting Documents

27.1 This policy should be interpreted and applied in relation to other related policies. A breach of one of these policies is likely to also be a breach of this policy. External policies are published on the Authority's website [3], Internal policies can be accessed from the Authority's intranet (Parcnet). These related policies include, but are not limited to:

a) Freedom of Information Publication Scheme (External)
b) ICT User Policy (Internal)
c) Information and Data Security Policy (Internal)
d) Safeguarding Statement (Internal)
e) Social Media Guidance (Internal)

27.2 The following supporting documents and forms are available from the Authority's website [3]

a) Freedom of Information Publication Scheme
b) Privacy Notice
c) Subject Access Request Form

27.3 The following supporting documents and forms are available from the Authority's intranet (Parcnet):

a) Staff Data Protection Guidance
b) Data Protection Register and Retention Schedule
c) Data Protection Impact Assessment Template
d) Data Breach Incident Form

28. Monitoring and Review

28.1 The implementation and effectiveness of this policy will be monitored and reviewed by the Authority's Data Protection Officer, Senior Management Team and Authority Members.

28.2 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 Audit and Corporate Services Committee.

28.3 This policy will be reviewed every 3 years or to respond to new data protection laws, guidance and best practice.

28.4 This policy has been prepared in line with current Information Commissioner's Office Guidance [2].

30. Reference

1	Wales Accord on Sharing Personal Information	http://www.waspi.org/home
2	Information Commissioner's Office Guidance	https://ico.org.uk/
3	Pembrokeshire Coast National Park Authority website	www.pembrokeshirecoast.wales
4	Pembrokeshire Coast National Park Authority's Overarching Privacy Notice	https://www.pembrokeshirecoast.wales/default.asp?PID=413
5	Authority's Subject Access Request form	www.pembrokeshirecoast.wales

31. Version History

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