DATA PROTECTION POLICY

1. INTRODUCTION

We are required by law to comply with the Data Protection Act 1998. This policy recognises the rights and obligations of the Pembrokeshire Coastal Forum CIC in relation to the management and processing of personal data.

The Data Protection Act requires anyone who handles personal data to comply with a number of important principles and it gives individuals rights over their personal data.

To comply with the Data Protection Act, data must be collected and used fairly, stored safely and not disclosed to any third party unlawfully.

The Data Protection Act states that;

Anyone who processes personal data must comply with the following 8 Data Protection Principles:

1. **Personal data shall be processed fairly and lawfully**
2. **Personal data shall be obtained only for one or more specified and lawful purpose(s) and used only in accordance with that purpose(s).**
3. **Personal data shall be adequate, relevant and not excessive.**
4. **Personal data shall be accurate and, where necessary, kept up to date.**
5. **Personal data processed for any purpose or purposes shall not be kept for longer than is necessary.**
6. **Personal data shall be processed in accordance with the rights of data subjects.**
7. **Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data.**
8. **Personal data shall not be transferred to a country or territory outside the European Economic Area.**

Every individual associated with us who processes or uses any personal data must abide by these principles at all times.
The Data Protection Act also provides individuals with important rights including the right to find out what personal data is held on computer and paper records (see 10. Subject Access Requests/Access to Records, for further information).

2. SCOPE

This policy applies to all electronic and paper based information and data, collected or accessed in relation to any PCF business activity, whether by employees, individuals or organisations under a contractual relationship.

This policy applies to ALL personal data created, received and maintained by employees in the course of their duties.

This policy applies to ALL personal data created, received and maintained by external parties on our behalf.

Other associated Policies:

- Information Governance Policy.
- IT Security Policy.
- Social Media Policy.

ROLES AND RESPONSIBILITIES

The Data Protection Act 1998 requires every Data Controller who is processing personal information to register with the Information Commissioners Office ("**ICO**").

The Data Controller in our case is the **"Pembrokeshire Coastal Forum".**

The Company is responsible for ensuring that the Information Governance function is addressed at the strategic level.

It is the role of the Board Members is to define the organisation's policy in respect of Information Governance, taking into account legal and business requirements. The Board is also responsible for ensuring that sufficient resources are available to support the requirements of the policy.

The Board has allocated the responsibility for data control to the ……. For the purpose of this policy and other related documents, this role will be referred to as the **"Records Manager".**

It is the responsibility of the Records Manager to maintain the notification to the ICO of personal data processed.

The Company is required to ensure that employees within their area of responsibility are made aware of the existence and content of this and other relevant policies. The Records Manager will inform the manager and employees of any changes or amendments to legislation and advise on implementation.

Data Protection enquiries and Subject Access Requests will be addressed to the Records Manager**.** However, this information will then be disseminated to and dealt with by the relevant "**Nominated Records Representative"**.

The Manager is responsible for ensuring that employees comply with legislation and organisational policies. The Manager will be expected to review Information Governance awareness during the appraisal process and arrange training if required.

All employees, whether permanent, temporary or contracted, are responsible for ensuring that they remain aware of the requirements upon them and conduct business in accordance with all applicable laws, regulations and contractual obligations.

4. PERSONAL DATA

Under the Data Protection Act, personal data is, or may be, personal data:

- About a living, identifiable individual;
- That relates to such an individual;
- Forming part of an accessible record;
- Held or intended to be held electronically;
- Held in a relevant filing system.

5. SENSITIVE PERSONAL DATA

Some data is classed as 'Sensitive' (within the terms of the Data Protection Act). This type of data is subject to further regulations under the Data Protection Act and can only be processed under certain circumstances.

Personal data becomes 'Sensitive' if it includes any of the following types of personal data about an identifiable, living individual:

- Racial or ethnic origin;
- Political opinions;
- Religious beliefs;
- Trade union membership;
- Physical or mental health;
- Sexual life;
- Commission of offences or alleged offences.

6. EMPLOYEE OBLIGATIONS

All employees, whether or not they physically create, receive or maintain personal data themselves, have an obligation to comply with the principles and requirements of the Data Protection Act.

In particular, employees must;

- Familiarise themselves with this policy.
- Work with their Nominated Records Representative or the Records Manager to ensure that requests for personal data are dealt with within 40 calendar days of receipt.
- Provide advice and assistance to individuals making Subject Access Requests for personal data in accordance with our guidelines.
- In relation to any telephone enquiries you should be careful about disclosing any personal data held by us. In particular you should:
    - o Check the caller's identity to make sure that information is only given to a person who is entitled to it.
    - o Suggest that the caller put their request in writing if you are not sure about the caller's identity and where their identity cannot be checked.

- o Refer to the Records Manager for assistance in difficult situations. No-one should be bullied into disclosing personal data.

- Contact the Records Manager where assistance is required.
- Manage all records in accordance with the Retention of Records section (refer to Appendix 1 of the Information Governance Policy) and make sure personal data is not retained for longer than necessary.
- Destroy in a secure fashion any records that have reached the end of their retention period (refer to Section 10 of the Information Governance Policy).
- Only process personal data to the extent to which they have been authorised.
- Advise the Records Manager of any new processing of personal data or any change in the processing of existing personal data.
- Comply with any implemented security procedures: o Ensure that any personal data held in any format, is kept securely;
  - o Ensure personal data is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party;
  - o Ensure that personal data is:
    - Locked in a filing cabinet/drawer;
    - If computerised, be password protected;
    - If kept on a CD/memory stick, be kept securely.
- Director, who authorise, processing of personal data by appropriate staff, are responsible for the monitoring of that processing.
- Ensure they comply with the principles and requirements of the Data Protection Act.
- Ensure all personal data provided to us is accurate and up to date.
- Only construct or maintain official files of personal data.
- Only process personal data to the extent to which they have been authorised.
- Be responsible for complying with any security procedures implemented.

Failure to Comply with this Policy

Violation of the standards, policies and procedures presented in this document by an employee will result in disciplinary action, from warnings or reprimands up to and including termination of employment. Claims of ignorance, good intentions or using poor judgement will not be used as excuses for non-compliance.

7. IMPLEMENTATION AND RETENTION

Data Protection enquiries and Subject Access Requests will be addressed to the Records Manager**.** However, this information will then be disseminated to and dealt with by the relevant Nominated Records Representative.

Personal data will be held in accordance with the Retention of Records appendix and destroyed in accordance with the Disposal of Records section, both contained in the Information Governance Policy. Issue Date: May 2013 Version 1.0

COLLECTION NOTICES

All employees are provided with a Contract of Employment that states the following:

> *"The Company reserves the right to collect, store and process personal data about its employees in so far as it is relevant to their employment. This includes sensitive data".*

Through signing a contract consent is given to the above. The collected data is securely stored within the department and is processed in accordance with the Data Protection Act 1998.

9. CONSENT OF DATA SUBJECTS TO THE PROCESSING OF SENSITIVE PERSONAL DATA

We may ask for personal data about an individual's health, particular health needs such as allergies, or any conditions such as asthma or diabetes. We will use such personal data in the protection of the health and safety of individuals or for any other legitimate reason. We may also ask for personal data about an individual's criminal convictions, race or gender. This is to ensure that we offer a safe place for everyone to work or may be to operate other policies, such as the Sickness Absence Policy or to provide monitoring data to external bodies.

Because such personal data is considered 'Sensitive', within the meaning of the Data Protection Act, all prospective employees will be asked to provide explicit consent to process particular types of personal data when an offer of employment is made. A refusal to give such consent without good reason may result in the offer being withdrawn.

10. SUBJECT ACCESS REQUESTS/ACCESS TO RECORDS

We recognise that all individuals (employees and external data subjects) have the right to be told whether we hold any personal data about them and as such we have established a procedure for responding to these requests. Individuals (or their representative) need to submit a written request to the Records Manager, Subject Access Request Form is available internally in the Employee Handbook. Any request must clearly state what personal data is being requested. The more clearly the request is defined, the more efficiently the request can be dealt with.

Written requests can be made by hand, post or email (see details below) and should be marked for the attention of the Records Manager.

Pembrokeshire Coastal Forum
2nd Floor, Pier House
Pembroke Dock
Pembrokeshire
SA72 6TR

Receipt of this request will be acknowledged immediately.

We reserve the right not to release any personal data where an exemption is applicable under the Data Protection Act. We will respond to each request as quickly as possible and will ensure that personal data is provided within the statutory period of 40 calendar days. However, this statutory period does not commence until:

- We have received suitable evidence of your identity;
- We are satisfied that the request is made by or with the knowledge and consent of the data subject.

Further instructions in relation to completing the Subject Access Request Form are provided in the Guidance Notes that accompany the form.

Access to Records

Under the Data Protection Act Part IV there are exemptions, most commonly as defined below, where an organisation is allowed to disclose personal information to a third party. Issue Date: May 2013 Version 1.0

Section 29 is an exemption that allows an organisation to give out personal information where the disclosure is for one of "crime" or "taxation" purposes:

- the prevention or detection of crime;
- the apprehension or prosecution of offenders; or
- the assessment or collection of any tax or duty or of any imposition of a similar nature;

and complying with the normal provision of the Data Protection Act would be likely to prejudice one of these purposes.

Under the exemptions, if an organisation has received a request from a third party for information constituting personal data, they may be able to release the data to the third party without the knowledge or consent of the data subject if the organisation which processes the date is satisfied that the exemption applies.

Organisations may receive requests for information under the exemption from the Police. However, the exemption does not specify who can make such requests; it is the purpose for which the disclosure will be made that is crucial in determining if the exemption applies.

In all cases, a Form, must be completed and submitted to the **"Records Manager"** using the contact details above. Request for Disclosure of Personal Data form which is available internally in the Employee Handbook.

11. COMPLIANCE

We will ensure that:

- There is always someone with specific responsibility for Data Protection in the organisation;
- All staff receives annual awareness of the Data Protection Act;
- Everyone managing and handling personal information understands that they are directly and personally responsible for following good Data Protection practice;
- Only staff that need access to personal information as part of their duties are authorised to do so; Issue Date: May 2013 Version 1.0

- Everyone managing and handling personal information is appropriately trained to do so;
- Everyone managing and handling personal information is appropriately supervised;
- Anyone wanting to make enquiries about handling personal information knows what to do;
- Queries about handling personal information are promptly and courteously dealt with;
- Methods of handling personal information are clearly described;
- A regular review and audit is made of the way personal information is managed;
- Methods of handling personal information are regularly assessed and evaluated;
- Performance on handling personal information is regularly assessed.

To assist in achieving compliance, we have:

- Appointed the Records Manager as the officer with overall responsibility for Data Protection within the organisation;
- Created a Data Protection Policy, providing detailed guidance on Data Protection procedures;
- Manager who will ensure compliance with the Data Protection Principles and adherence to the Policy in his areas of responsibility.

We will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

- Data Processors are appropriately trained in the handling of personal data;
- Paper files and other records containing personal/sensitive data are kept in a secure environment;
- Personal data held on computers and computer systems is protected by the use of secure passwords which, where possible, have forced changes periodically;
- Individual passwords are not easily compromised. Issue Date: May 2013 Version 1.0

If and when, as part of their responsibilities, individuals collect information about other people, they must comply with the guidance set out in our Data Protection Policy. No one should disclose personal data outside this guidance or use personal data held on others for their own purposes.

12. FURTHER INFORMATION

More information about the Data Protection Act 1998 is available on the ICO website at: www.informationcommissioner.gov.uk

13. POLICY REVIEW

This policy will be reviewed at least once every year and, if necessary, amended to ensure continued compliance with the Data Protection Act.

14. COMPLAINTS

Complaints relating to Data Protection should be submitted in writing to the Records Manager by post or email (see details below).

Pembrokeshire Coastal Forum
2nd Floor, Pier House
Pembroke Dock
Pembrokeshire
SA72 6TR

Receipt of the complaint will be acknowledged immediately and the Records Manager will investigate the complaint in liaison with the Nominated Records Representative**.** A response shall be sent within 21 calendar days.

Individuals wishing to withdraw their complaint should contact the Records Manager or Nominated Records Representative in writing as above. Receipt of this request will be acknowledged immediately and action taken where appropriate (or responded to) within 21 calendar days. Issue Date: May 2013 Version 1.0

Once the complaint has been dealt with, if the complainant remains dissatisfied with the outcome, they may seek an independent review from the ICO. This is the independent body responsible for overseeing the Data Protection Act. The ICO can be contacted in writing at:

The Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

15. POLICY AWARENESS

A copy of this Policy Statement will be available to all new employees. Existing employees and any relevant third parties will be advised of the Policy or any subsequent revisions. All employees and relevant third parties are to be familiar with and comply with this Policy at all times.