DATA PROTECTION POLICY
October 2012

As individuals, we want to know that personal information about ourselves is handled properly, and we and others have specific rights in this regard. In the course of its activities Northumberland Inshore Fisheries and Conservation Authority (the Authority) will collect, store and process personal data, and it recognises that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

The types of personal data that the Authority may be required to handle/include information about current, past and prospective members and employees, suppliers, officials, fishermen, and any other person or member of the public with whom it communicates. The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 1998 (the Act) and other regulations. The Act imposes restrictions on how the Authority may process personal data, and a breach of the Act could give rise to criminal sanctions, financial penalties and compensation payments as well as bad publicity.

STATUS OF THE POLICY

This Policy sets out the Authority's rules on data protection and the eight data protection principles contained in it. These principles specify the legal conditions that must be satisfied in relation to the obtaining, handling, processing, transportation and storage of personal data.

The Authority's Data Protection Compliance Manager is responsible for ensuring compliance with the Act and with this policy. The Data Protection Compliance Manager is Michael H. Hardy LL.B, Chief Executive, Tel. No. 01670 731 399, email michael.hardy@nifca.gov.uk. Any questions or concerns about the interpretation or operation of this policy should be taken up in the first instance with the Data Protection Compliance Manager.

This policy is not part of the contract of employment and the Authority may amend it at any time. However, it is a condition of employment that employees and other workers who obtain, handle, process, transport and store personal data will adhere to the rules of the policy. Any breach of the policy will be taken seriously and may result in disciplinary action.

Any worker who considers that the policy has not been followed in respect of personal data about themselves or others should raise the matter with the Authority's Data Protection Compliance Manager in the first instance.

DEFINITION OF DATA PROTECTION TERMS

Data is recorded information whether stored electronically, on a computer, in paper-based filing systems.

Data subjects for the purpose of this policy include all living individuals about whom the Authority holds personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in the possession, or likely to come into the possession, of the Authority). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal). It can even include a simple e-mail address.

Data controllers are the people or organisations who determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. The Authority is the data controller of all personal data used in its business.

Data users include workers whose job involves using personal data. Data users have a duty to protect the information they handle by following the Authority's data protection and security policies at all times.

Data processors include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on the Authority's behalf.

Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

DATA PROTECTION PRINCIPLES

Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

- Processed fairly and lawfully.
- Processed for limited purposes and in an appropriate way.
- Adequate, relevant and not excessive for the purpose.
- Accurate.
- Not kept longer than necessary for the purpose.
- Processed in line with data subjects' rights.
- Secure.

- Not transferred to people or organisations situated in countries without adequate protection.

FAIR AND LAWFUL PROCESSING

The Act is intended not to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is (in this case the Authority), the purpose for which the data is to be processed by the Authority, and other information which makes the particular processing fair.

For personal data to be processed fairly and lawfully, certain specific conditions also have to be met. These include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interests of the data controller or the party to whom the data is disclosed, which is not overridden by prejudice to the data subject's rights, freedoms and legitimate interests. When sensitive personal data is being processed, additional conditions must be met. In many cases the data subject's explicit consent to the processing of such data will be required.

PROCESSING FOR LIMITED PURPOSES

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Act. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.

ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

ACCURATE DATA

Personal data must be accurate and kept up to date where necessary. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed, except where required as an audit trail.

TIMELY PROCESSING

Personal data should not be kept longer than is necessary for the purpose for which it was collected. This means that data should be securely destroyed, or erased from the Authority's systems when it is no longer required, or it may be anonymised.

PROCESSING IN LINE WITH DATA SUBJECTS' RIGHTS

Data must be processed in line with data subjects' rights. Data subjects have a right to:

- Request access to any data held about them by a data controller.
- Prevent the processing of their data for direct marketing purposes.
- Ask to have inaccurate data amended.
- Prevent processing that is likely to cause substantial and unwarranted damage or distress to themselves or anyone else.

DATA SECURITY

The Authority must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.

The Act requires the Authority to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if he agrees in writing to use the personal data only on the Authority's instructions and to comply with the security requirements in the Act.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

- **Confidentiality** means that only people who are authorised to use the data can access it.
- **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.
- **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on the Authority's central computer system instead of individual PCs.

Security procedures include:

- **Entry controls.** Any stranger seen in entry-controlled areas should be reported.
- **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.) Personal data should not be taken out of the office.
- **Methods of disposal.** Paper documents should be shredded. Floppy disks and CD-ROMs should be physically destroyed when they are no longer required. Hard disks (which are in photocopiers as well as PCs and laptops) should be securely disposed of by a specialist company.
- **Equipment.** Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended. Computer media such as laptops and USB sticks

containing personal data must be encrypted. Emails sending personal data should also be encrypted.

DATA EXPORT

The Authority must ensure that personal data are not transferred to a country or territory outside the European Economic Area (the EEA) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. The EEA means the EU member states, Norway, Iceland and Liechtenstein. This means data users should not transfer personal data to countries or territories outside the EEA without referring to the Data Protection Officer for assistance.

DEALING WITH SUBJECT ACCESS REQUESTS

A formal request from a data subject for information the Authority holds about them must be made in writing. Employees who receive a written request should forward it to the Data Protection Compliance Manager immediately.

DEALING WITH THIRD PARTY REQUESTS

When receiving telephone enquiries, employees should be careful about disclosing any personal information held on the Authority's systems. In particular they should:

- Check the caller's identity to make sure that information is only given to a person who is entitled to it.

- Ask the caller to put their request in writing where the employee is not sure about the caller's identity and where their identity cannot be checked.

- Refer to the Data Protection Compliance Manager for assistance in difficult situations. Employees should not be bullied into disclosing personal information.