

**Date: 25 September 2007**

**Report: DATA PROTECTION POLICY**

**Purpose of the report**

1. To ask Members to consider and approve the attached draft Data Protection Policy for the Authority.

**Strategic Planning Framework**

2. The information and recommendation(s) contained in this report are consistent with the Authority's statutory purposes and its approved strategic planning framework:
  - Best Value Performance Plan: Support and empower staff to provide professional, positive and proactive services to the public.
  - Core Value Integrity: Our relationships with the public, partners and each other will be built on honesty, transparency, equality, impartiality and consistency.

**Background**

3. Data Protection has been the subject of legislation for over 20 years now, the current statute being the Data Protection Act 1998, under which many sets of detailed Regulations have been made. There are important interactions between this legislation and the Freedom of Information Act 2000.
4. The Authority does not currently have a Data Protection Policy. It is important that it should, both to demonstrate the seriousness with which it regards its legal obligations, and to provide guidance to staff and members in this often difficult area. The Information Commissioner (who polices both data protection and freedom of information legislation) publishes a guide to auditing compliance: the first audit objective is that the organisation has a system which exists and is compliant, and the primary evidence of this is the organisation's data protection policy. The Information Commissioner has various investigatory powers, and it is clear that he would expect organisations to have a data protection policy.
5. A policy for the Authority has therefore been drafted, and the Senior Management Team now recommend it for approval (see Appendix 1).

## **Key Issues**

6. Without being unrealistically aspirational, we do have to get the fundamentals right, which means complying with our registration conditions, making sure everyone has read and has access to the data protection principles, and responding correctly to subject access requests. We also need to realise that carelessness in this area can get the Authority into considerable difficulties. A basic awareness briefing is therefore being provided to all staff of the Authority (through Departmental meetings), and more detailed training will also be provided for a target group of staff who need to have a deeper understanding.
7. The policy is the framework, and contains helpful guidance on the data protection principles, and how to deal with subject access requests. There are various actions that need to be taken to ensure full compliance with the law and with this new policy, and these are summarised in Appendix 2.
8. Members will note that one of these actions is for me to give guidance to Members themselves about the implications for them of the Data Protection Act, and that I will do shortly.

## **Conclusion**

6. Members are asked to consider this report as a framework and programme of work to ensure that the Authority's working practices are compliant with data protection legislation.

## **RECOMMENDATION**

7. That the Data Protection Policy attached at Appendix 1 be formally approved.
8. Subject to that approval, that it be publicised to staff and included in the Authority's corporate policy database.
9. That the individuals named in Appendix 2 be tasked with carrying out the work identified, to bring practice into line with the policy.

**Richard Daly**  
**Solicitor / Monitoring Officer**

10 September 2007

Background documents:  
None

**YORKSHIRE DALES NATIONAL PARK AUTHORITY**

**Data Protection Policy**

**Key Statement**

**The Yorkshire Dales National Park Authority acknowledges that it holds personal data on trust and that harm may arise if that data is misused.**

**THEREFORE:-**

**We will employ good practice in all matters concerned with the use of personal data.**

**We will ensure that such data is kept secure and is used only for properly authorised purposes.**

**We will ensure that the rights of data subjects are properly respected.**

**In these and other respects we will seek to adhere at all times to the requirements of the Data Protection Act 1998 and other relevant legislation.**

**1. DEFINITION AND RESPONSIBILITIES**

- 1.1 These procedures implement the requirements of the Data Protection Act 1998 together with relevant regulations, and guidance from the Information Commissioner. They relate to how we deal with personal data: that is, ANY information about a living individual.
- 1.2 Overall responsibility for data protection issues at senior management level rests with the Solicitor / Monitoring Officer. Responsibility for day to day issues, such as progress chasing subject access requests, rests with the Secretariat Administrator, who is the designated Data Protection Co-ordinating Officer.
- 1.3 Responsibility for all issues concerned with computer security lies with the Head of Finance and Resources.

**2. CONTEXT**

- 2.1 The Data Protection Act 1998 (DPA 1998) covers all personal information about living identifiable individuals, whether the information is held on computer or not. It includes expressions of opinion about individuals, and information about our intentions towards them. The Act requires a pro-active approach on behalf of both data controllers and staff. The requirements of the DPA 1998 have also to be seen in the context of other relevant legislation, in particular the Human Rights Act 1998 and the Freedom of Information Act 2000.

- 2.2 The Yorkshire Dales National Park Authority (YDNPA) is registered under the DPA 1998 and annual notification is given to the Information Commissioner by the Senior IT Officer.
- 2.3 The DPA 1998 defines some data as particularly sensitive: eg political opinions, racial origin, religion, health, criminal records. YDNPA does hold some sensitive personal data, particularly in relation to staff: sickness records, occupational health reports, details of trade union membership, ethnic origin and the results of Criminal Records Bureau (CRB) checks (the latter are undertaken under the terms of a separate policy designed to ensure compliance with legal requirements and the protection of children and vulnerable adults). We are allowed to process sensitive personal data in connection with the Authority's role as an employer, but must not use it for other purposes without the explicit consent of the person concerned. The equal opportunities monitoring form used in recruitment asks for explicit consent to processing of the information given, and the information held about staff members is available to the person concerned.

### 3. PRINCIPLES

- 3.1 Data Protection practice is informed by the following **eight Data Protection Principles**, defined in Schedule 1 of the DPA 1998 and described here:
- 3.1.1 Personal Data shall be processed fairly and lawfully and, in particular, shall not be processed unless certain conditions (set out in the Act) are met.
- 3.1.2 Personal Data shall be obtained and processed **only** for the purposes specified in the organisation's data protection registration, and shall not be further processed in any manner incompatible with those purposes.
- 3.1.3 Personal Data shall be adequate, relevant and not excessive in relation to the specified purposes.
- 3.1.4 Personal Data shall be accurate and, where necessary, kept up to date.
- 3.1.5 Personal Data shall not be kept longer than is necessary for the specified purposes.
- 3.1.6 Personal Data shall be processed in accordance with the defined rights of Data Subjects.
- 3.1.7 Appropriate technical and organisational measures shall be taken to protect Personal Data.
- 3.1.8 Personal Data shall not be transferred to a country outside the European Economic Area
- 3.2 Data Protection is a shared responsibility between all individual members of staff and the Authority.

**All staff** (with actual or potential access to personal data) hold a personal responsibility for understanding and adhering to the requirements of this policy.

**The Authority** has corporate responsibilities for proper registration, to ensure that staff are properly informed, to put in place proper systems and procedures and to deal properly with any incidents that may arise.

#### 4. AIMS

The aims of YDNPA in relation to data protection are:

- 4.1 To ensure that the requirements for systems and procedures are properly understood and implemented.
- 4.2 To ensure that the Authority only uses personal data for legitimate purposes.
- 4.3 To ensure that all staff understand their responsibilities and the Authority's responsibilities.
- 4.4 To ensure that the rights of data subjects are properly respected.
- 4.5 To enable YDNPA to maintain and comply with an accurate registration.
- 4.6 And in any other respect, to ensure that YDNPA satisfies the requirements of the DPA 1998 and adheres to good data protection practice.

#### 5. PRINCIPLES IN PRACTICE

This section is structured according to the eight principles of Data Protection described in paragraph 3.1 above.

##### 5.1 Fair and Lawful Processing

- 5.1.1 We will give a notification to persons about whom we are seeking to (or do in fact) obtain personal data that we intend to process. The notification will explain what types of information we hold, what we use it for and what their rights are to access that information. We will normally provide the notification on the first occasion that we make contact.
- 5.1.2 Before we share personal data with others (ie persons who are not Members or Staff of the Authority), we will agree with the other party a protocol which gives details of what procedures to follow, in particular to identify any consent needed from data subjects or requirements to inform data subjects.
- 5.1.3 Whenever data is provided to an agency or individual outside of the Authority, **details of the disclosure must be recorded** on the appropriate record (computer record, personnel file etc).

5.1.4 Changes to the use of personal data and new arrangements for sharing or providing data **may not take place** without prior reference to the Solicitor / Monitoring Officer to ensure that Data Protection issues are properly addressed.

## **5.2 Obtained and processed only for specified purposes**

5.2.1 The Senior IT Officer will ensure that the registration is kept up to date. This lists the purposes for which personal data is held by YDNPA (see Annex D).

5.2.2 **Use of data for purposes other than those described in the YDNPA data protection registration is not allowed.** Any proposed additional uses must first be referred to the Senior IT Officer for consideration to be given to the need to amend our registration.

## **5.3 Adequate, relevant and not excessive**

We will take care to ensure that unnecessary data is not held. YDNPA rules on the retention and destruction of records are attached (Annex B).

## **5.4 Accuracy and currency**

5.4.1 All staff must record information accurately as soon as they receive it, take reasonable steps to validate such information and then apply (and record) any corrections or alterations as they become known. Where corrections are required (NB: individuals have the right to insist that information about them which is wrong is duly corrected) then others who also hold or have received that information must be informed.

5.4.2 Where there is a dispute with the data subject about the accuracy of a piece of data then, where agreement cannot be reached, it may be appropriate to record the dispute rather than alter the data.

## **5.5 Retention**

Retention periods for all categories of data are as identified in our retention and destruction of records rules. Procedures will be developed to ensure that data is destroyed once the retention period expires.

## **5.6 Rights of Data Subjects**

5.6.1 Requests for data subject access will only be accepted in writing (hard copy not email), signed by and addressed from the current abode of the data subject.

5.6.2 In order to discourage mischievous and unnecessary requests we will normally charge the maximum fee allowed (currently £10). However, the Data Protection Co-ordinating Officer will consider waiving the fee whenever evidence is presented indicating that the fee will cause particular hardship or problems to the data subject.

- 5.6.3 All requests for data subject access must be acknowledged in writing and then notified to the Data Protection Co-ordinating Officer who will advise on how to respond.
- 5.6.4 Procedures have been developed to ensure that the satisfaction of access requests is expedited, that the maximum appropriate data is always provided (as the law requires) but that all data to be provided is first properly reviewed to ensure that inappropriate information is not supplied. The procedures are attached at Annex C.

## **5.7 Security Measures**

- 5.7.1 We will adhere to best practice for the design and security of computer systems, the design and security of working areas, the security of filing systems and the security of premises.
- 5.7.2 All users of YDNPA computer systems will be required to adhere to any current policy or procedure covering the authorisation of user names and the security of passwords. Access to files and folders held on computer will be arranged by the Senior IT Officer, bearing in mind data protection requirements.

## **5.8 Transfer outside the European Economic Area (EEA)**

For the purposes of YDNPA policy it is clearer for all concerned if we use the United Kingdom rather than the EEA as the territorial limit for data transfer. Therefore personal data will **NOT** be taken or transferred out of the United Kingdom (whether on paper or in electronic form) except with the specific written authority of the Monitoring Officer. Such authority will only be given on a case by case basis and then normally only where that transfer is necessary for reasons of substantial public interest or is required by statute.

## **6. MONITORING AND EVALUATION**

- 6.1 An audit will take place at least once every three years, the details of which will be developed by the Data Protection Co-ordinating Officer.
- 6.2 A report will be submitted to the Senior Management Team annually by the Data Protection Co-ordinating Officer, reviewing the extent to which implementation of this policy has been achieved; together with information on the number and outcome of subject access requests received.

## **7. STAFF DEVELOPMENT AND TRAINING**

- 7.1 This policy will be issued to all staff.
- 7.2 All staff will be provided with a simple checklist (see Annex A) that ensures they appreciate the key messages.

7.3 The Monitoring Officer is responsible for ensuring that staff who deal with personal data receive appropriate training in data protection requirements.

This policy was agreed by the Yorkshire Dales National Park Authority on 25<sup>th</sup> September 2007, and will be reviewed in September 2010.

<b>STOP</b>	<b>THINK</b>
<b>ACT</b>	<b>RECORD</b>

Annex A

**Yorkshire Dales National Park Authority**

**Care of Personal Data**

**A Quick Check-List**

- **NEVER** give personal information about anyone to **anyone** outside the Authority **unless** you are absolutely certain about their credentials, their reasons for seeking the information, their entitlement to the information and that you have a right to disclose that information.
  
- **Always respond neutrally** to telephone requests for information about an individual. An answer such as “I will look into your request and get back to you” is **always** appropriate. An answer such as “I will look at their file and get back to you” is **risky**. Even such an apparently innocuous answer has already given away personal information.
  
- **Always obtain the number and name** of a caller seeking personal data and get back to them to ensure that they really are from the agency they purport to be from.
  
- **Whenever you disclose** personal information, **record the full circumstances of the disclosure** on the relevant case or staff record.
  
- **Any information disclosed** must be **relevant** to the reason for disclosure, **necessary** to achieve the purpose of the disclosure, **not excessive** and must be the **minimum necessary** in each case.
  
- **Don't put** personal information onto **floppy disks, CDs or laptops**.
  
- **NEVER disclose** your **password** or let anyone else use your **username**.
  
- Except in the exercise of their legal rights (eg to inspect papers relating to planning applications) **Don't give anyone not employed** by the Authority **access to manual files or computer systems** which would allow them to access personal information, unless they have been properly authorised by a senior manager.



## YORKSHIRE DALES NATIONAL PARK AUTHORITY

### Document retention and destruction rules

The Data Protection Act 1998 requires that personal data should not be retained for longer than is necessary. To qualify as personal data it has to be information relating to a living individual who is identified or who can be identified.

The length of time for which personal data may be kept depends on why it is kept. It is important when retaining any computer or paper record, to ensure that it is clearly marked to show when it was last updated and the earliest date when it may be deleted. Records which are no longer being updated should be marked as such and show a review date at which time records should be deleted or a new review date fixed.

The following retention periods should normally be adhered to; but the table below should be used as a guideline and not followed slavishly where legislation or other circumstances dictate a different period than that recommended. It is necessary to remember that the Authority is a public body, and needs to keep some records for reasons of enabling the public to exercise rights of access to information, and/or to maintain an historical record of its activities.

Information relating to	Suggested retention period
Authority and Committee meetings; minutes, reports, agendas etc	In perpetuity
Authority policies, strategies, annual reports etc	In perpetuity
Legal documents: contracts, grants, papers related to litigation / public enquiries, legal agreements, insurance claims.	6 years after expiry, unless of general public interest, in which case consider offering to public archives
Health & safety records, accident books etc	6 years after closure
Planning applications and applications for legal consents	Name, address, nature of application & decision: in perpetuity. Financial / medical information: 20 years.
Enforcement cases etc	Name, address, nature of action & outcome: in perpetuity. Other information: 20 years.
CRB check results	6 months from receipt
Staff records – unsuccessful applicants.	6 months after unsuccessful job application.

Staff records	6 years after leaving Service, except for pensions information, which is kept separately and retained for the lifetime of the person.
Volunteers	6 years after ceasing to be a Volunteer
Authority Members	6 years after membership ceases, apart from name, contact details, and record of service on the Authority, which will be kept in perpetuity.
Any other individuals with whom we have financial dealings (including recipients of grants and other assistance).	6 years after payments cease.
Complaints, Ombudsman references and allegations of breach of the code of conduct.	6 years after final reply to complainant.
Individuals, but relevant to Dales history, culture etc.	In perpetuity, subject to the consent of the individual, and Dales Countryside Museum (DCM) policies on collecting.
Historic Environment Record, publicly accessible registers, documents relating to listed buildings	In perpetuity
Events publicity mailing	2 years from the event
Education enquiries	6 months
Education / outreach / events group visits	6 years from the event
Evaluation / leaders report form	One year from the event unless accident information recorded, in which case 6 years
Contact details of group organisers	2 years from last event

#### NOTES :

1. The Pension Fund also has responsibility for holding information on retired staff.
2. Files sent for storage to Iron Mountain are subject to an agreement which compels Iron Mountain to keep personal information confidential.
3. Data which was originally Personal Data and which is information about a person who is still alive can be retained indefinitely for research, training, statistical or any other purposes so long as any pieces of information which enable the individual to be identified are removed. It is also important that if data are retained, for example

for research purposes, the identity of any individual who is the subject of that data cannot be obtained from the product of the research. Remember that in a sparsely populated area someone from that area may immediately recognise the data as relating to a specific individual. Any deleted information removed in order to depersonalise the data cannot be retained since it might enable the original record to be reconstituted and individuals identified. Were that to be possible the data would never have ceased to be personal data. Similarly, it would not be acceptable to encrypt fields used to identify the individual if the cipher key is retained so that the information could readily be decrypted.

When a file is closed, a date for its retention will be placed on the file. At that date, the file will be reviewed by the relevant Head of Department (or officer authorised by him/her), who will confirm that it is to be destroyed, or record (with reasons) why and until when it should be retained.

Personal data which is no longer relevant for the purpose for which it was collected, or which has passed its retention period, will be destroyed. Paper records will be shredded and computer records will be deleted from systems so that they cannot be retrieved or recreated, either by the Authority or anyone else.



## YORKSHIRE DALES NATIONAL PARK AUTHORITY

### A Guide to dealing with subject access requests under the Data Protection Act 1998

1. The Data Protection Act 1998 gives rights to individuals who wish to know if personal data about themselves is held by an organisation. One of the rights is to make a subject access request: that is, a request to be told whether any personal data is held about them, and if so to be provided with a copy of that data.
2. Each Department within the Authority is responsible for dealing with and responding to requests which relate to its area of work. However, you also need to involve the Data Protection Co-ordinating Officer (Lesley Knevitt).
3. If you receive a request for personal information, check the following:
  - (a) Is the person asking for information about themselves (or do they have a signed document authorising them to ask on behalf of someone else)?
  - (b) Is the request for personal data – ie data about a living individual who can be identified from the data?If the answer to either of these questions is no, there is no valid request under the Data Protection Act. If the person wants information which is not personal data, refer the request to the officer who deals with that area of work.
4. All requests for access to personal data must be accompanied by a £10 fee. If this has not been sent, ask for it, and take no further action until it is received.
5. Once a valid request has been received, together with the fee, this should be acknowledged in writing and the Data Protection Co-ordinating Officer should be informed immediately.
6. The Data Protection Co-ordinating Officer will then contact you to review the matter, and advise how to deal with it. The Authority has 40 days, from the date the request and payment were made, to give access to the personal data.
7. The most frequent problem in relation to giving access to personal data is that it may contain information about people other than the person who is asking to see it. Where this is the case, consideration must be given to excluding the third party information from what is disclosed. Where this is not possible, the third party must be contacted where possible, and their consent to disclosure sought. Where this cannot be obtained, consideration has to be given to whether it is reasonable to disclose the data.
8. The Data Protection Co-ordinating Officer will consult the Monitoring Officer where necessary in connection with disclosure requests.
9. ***Under no circumstances*** should you ever delete, alter, remove, or otherwise tamper with personal data because a subject access request has been made. The only changes which may be made between receipt of the request and giving access to the information are normal processes such as updating the data to deal with ongoing events.
10. The Data Protection Co-ordinating Officer will advise on matters such as how access is to be given, how to exclude third party information etc.

YDNPA Data Protection Registration

YDNPA is registered to process personal data for the following 12 purposes:

1. Staff Administration: Appointments or removals, pay, discipline, superannuation, work management or other personnel matters in relation to YDNPA staff.
2. Accounts and Records: Keeping accounts related to any business or other activity carried on by the Authority, or deciding whether to accept any person as a customer or supplier, or keeping records of purchases, sales or other transactions for the purpose of ensuring that the requisite payments and deliveries are made or services provided by or to the Authority in respect of those transactions, or for the purpose of making financial or management forecasts to assist the Authority in the conduct of any such business or activity.
3. Property management: The management and administration of land, property and residential property and the estate management of other organisations.
4. Providing Leisure and Cultural Services.
5. Assessment and Collection of taxes and rates (this purpose would not appear to be necessary for YDNPA).
6. Administration of benefits, grants and loans.
7. Licensing and regulatory activity, including planning and highways functions, investigation, prosecution, preparation and serving of enforcement notices
8. Crime prevention and detection (we do have a legal duty to co-operate in this).
9. Corporate functions, including Authority and Committee meetings, liaison with other public bodies, economic and community development, audit, best value studies, satisfaction surveys, complaints procedure, emergency planning, and legal services.
10. Non commercial activities including providing services to parish and other councils, maintaining public grounds, administration of grants and concessionary schemes, and provision of services for voluntary sector projects.
11. Other services such as administration of car parks and insurance administration.
12. Advertising, Marketing, Public Relations, and General Advice Services, including promotional and other publicity campaigns, promotion of Authority services, general advice to the public, and promotion of local tourism.

Practical issues that need attention

1.	Inform all current staff, members and volunteers what data we hold about them (ie what types of information, not the information itself), and their rights of access to it.	Personnel Section / Secretariat / Volunteers Co-ordinator.
2.	Include a similar statement in the induction pack given to all new starters.	Personnel Section
3.	Consider and introduce arrangements to notify service users whose data we intend to process what information we hold, and their rights of access to it. This should cover inclusion of an appropriate endorsement* on forms etc which are designed to elicit personal information, plus notification to others whose information we have obtained in the past, if we obtained it without such a statement and we still use it.	Head of Planning Head of Park Management Head of Conservation & Policy
4.	Ensure that any “competitions” etc, either on the website or in publications contain clear conditions about the use to which the data submitted by entrants will be put, and that by entering they consent to that.	Communications Team
5.	Introduce systems of marking files with a destruction date when they are closed.	All Heads of Department
6.	Consideration of the implications for DCM	Solicitor / Monitoring Officer & Museum Manager
7.	Staff awareness raising – through Departmental meetings	Solicitor / Monitoring Officer
8.	Training for staff who need more detailed knowledge	Solicitor / Monitoring Officer
9.	Develop details of data protection audit (? Ask internal audit service to do this)	Member Services Officer (as DPA Co-ordinator)
10.	Give guidance to Members about the application of Data Protection legislation to them.	Solicitor / Monitoring Officer

The completion date for the above actions is 31 March 2008.

\* these may need to be customised to particular uses; but here is an example that we currently use on email contacts for education enquiries:

**DATA PROTECTION ACT**

The contact details you have provided will be stored in the Yorkshire Dales Education Network database and will be used only for those purposes for which the information was supplied. Personal information used to service education enquiries will be removed no later than six months following use, while information relating to the subject only will be held to compile statistical information about our activities.

You can request access to your ‘data subject’ details which we hold by writing to The Education Service, YDNPA, Colvend, Grassington, Skipton BD23 5LB