Veritau
Assurance Services for the Public Sector

# Information Governance Follow-Up

# Peak District National Park Authority

# Internal Audit Report 2015/16

Business Unit: Peak Corporate Services
Responsible Officer: Director of Corporate Services
Service Manager: Head of Information Management
Status: Final
Date Issued: 17th February 2016
Reference: 69190/002b

| | P1 | P2 | P3 |
|---|---|---|---|
| **Actions** | **0** | **0** | **2** |
| **Overall Audit Opinion** | High Assurance | | |

PEAK DISTRICT NATIONAL PARK

# Summary and Overall Conclusions

## Introduction

Information is one of the most valuable assets held by any organisation. The Data Protection Act 1998 (DPA), Freedom of Information Act 2000 (FOIA) and Environmental Information Regulations 2004 (EIR) place obligations on public authorities which handle personal data and requests for information. Organisations need to ensure that data are held securely and remain accessible only to those with a need to view them, while also meeting transparency requirements.

Compliance with the Acts and Regulations is monitored by the Information Commissioner's Office (ICO). The ICO has the power to levy fines of up to £500,000 for non-compliance with data protection principles.

Therefore an audit of information governance was undertaken in October 2014, which examined Information Governance, Data Protection and Freedom of Information procedures, to support additional work on disaster recovery and some technical aspects of data security, which was undertaken and reported separately (Ref. 69180/001).

An overall audit opinion of "moderate assurance" was given.

## Objectives and Scope of the Audit

The objective of the audit was to review progress towards the completion of the actions raised in the 2014-15 Information Governance audit (Report Ref: 69140/001).

The purpose of the original audit was to provide assurance to management that procedures and controls within the system ensured that:

- staff were adequately trained in DPA, FOIA and EIR issues;
- DPA, FOIA and EIR roles and responsibilities were clear;
- data breaches were handled in accordance with the DPA; and
- information requests made under the Acts and Regulations were handled appropriately.

## Key Findings

The original audit report included seven actions which PDNPA had agreed to implement, in order to address the findings of the report.

Of the seven agreed actions, most of which included several elements, five have been fully implemented. The remaining two agreed actions have been substantially implemented, and the authority is working towards completing the outstanding elements and has identified reasonable target dates for the completion of these remaining actions.

The following elements of actions have not yet been fully implemented:

- training self-assessment questionnaires to be assessed by management and rolled out to staff; and
- named information asset owners are to be introduced.

## Overall Conclusions

It was found that the arrangements for managing risk were very good. An effective control environment appears to be in operation.

## 1 Senior management responsibility for information governance

| 1 Original Findings | Original Risk |
|---|---|
| PDNPA's Information Management Policies Framework is the key document covering information governance and data management principles. However, it does not assign overarching responsibility to a senior individual officer, and a SIRO is not named. The Framework directs anyone with queries to the Head of Information Management or ICT, and also states that "heads of service are directly responsible for implementing the policies within their business areas, and for ensuring staff work within them".<br>There is no specified role for a lead member of the Authority, as the Authority does not allocate any operational roles in information management to Members. | Ineffective information governance, leading to fines from the ICO. |

### 1.1 Original Agreed Actions

Although we believe the role of the SIRO is currently adequately covered through the roles of the Head of Information Management, the Director of Corporate Resources and the Records and Information Manager we will strengthen these arrangements by updating the job description of the Head of Information Management to give this post the lead role to be introduced with the appointment of a new Head of Information Management in January 2015. The new post holder will work with the Director of Corporate Resources and the Information Management Steering Group to ensure he/she has appropriate access to the management team. This is a similar model to the way the statutory CFO and MO roles operate.

### 1.2 Current Position

The role of SIRO has been formally added to the head of information management job description.

The initial plan was to implement the SIRO role following the creation of IAS (as per the information management strategy) though as this was delayed by an organisational restructure the SIRO role has been introduced ahead of the IAOs.

### 1.3 Agreed Actions

No further action required.

## 2 Training and guidance

| 2 Original Findings | Original Risk |
|---|---|
| Staff have to complete twelve questions in an online survey after they have read the Information Management Policies Framework - this is part of the induction programme for new starters. The Head of Information Management advised that around 20 users have not completed this.<br><br>Members do not have to complete the survey, and only 5 out of 30 members attended an internal FOI/EIR briefing for the Members given in June 2012 by the Records and Information Manager. Some officers, including senior managers and Customer Services staff, are expected to undertake specialist training, and this was offered in 2012, but has not been repeated. This means that several members of staff who have joined the Authority since then have not had the training which was deemed necessary for their role and/or predecessors.<br><br>The Information Management Policies Framework does not assign overall responsibility to an individual for ensuring that all relevant training is provided and completed. | Poor understanding of legislation and personal obligations, causing information security breaches, leading to the imposition of fines or other penalties by the ICO. |

### 2.1 Original Agreed Actions

We do not believe there is evidence that staff and members have a poor understanding of the legislation and personal obligations relating to data management. The current arrangements and procedures identify issues quickly and allow risks to be managed efficiently and effectively. We do accept, however, that we could improve training and guidance procedures by taking the following actions:

- Remind staff of guidance notes and procedures available on the intranet and provide an on line self-assessment tool to test basic knowledge

- Introduce a training programme for members, new staff and any anyone failing to pass the self-assessment test. This will cover FoI/EIR, Data Protection and the fundamentals of data management. We will consider with management team whether this training should be mandatory.

- Train all staff in use of the HUB – electronic document management systems for holding and managing all business records.

- Ensure all staff have completed the on-line Policy Framework questionnaire
- Assign responsibility for training to the Records and Information Manager with support from management team and line managers.

## 2.2 Current Position

Multiple reminders have been sent to staff as well as update notifications regarding specific changes to the policy document.
The self-assessment questionnaire has been abandoned in favour of a new training module which has been developed. This is to be assessed by management team during February 2016 and rolled out to staff during March – June 2016.

Three audits have been completed, and all staff have now completed the online policy framework questionnaire.

Responsibility for training has been assigned to the information and records manager. This is being further strengthened by a change to the job description and person specification.

## 2.3 Agreed Actions

Self Assessment questionnaire to be assessed by management team during February 2016 and rolled out to staff during March – June 2016.

| | |
|---|---|
| **Priority** | 3 |
| **Responsible Officer** | Head of Information Management |
| **Timescale** | 30th June 2016 |

## 3 Record retention

| 3 Original Findings | Original Risk |
|---|---|
| The Information Management Policies Framework covers "Retention and Disposal of Information", and refers staff to the "Guidelines for Retention" on for further details. In referring to the "Guidelines for Retention", the Framework states that they "should be considered once a file is 'closed' i.e. no further action is required or expected".<br><br>The Authority holds all records on site, and due to various restructures and changes in building use, many hard copy documents which were no longer required have been destroyed.<br><br>However, there is no process to trigger the destruction of hard copy documents, and the Framework and Guidelines do not assign responsibility for ensuring that destruction takes place. The Authority is working towards a comprehensive electronic document management system, and this will include the ability to prompt data owners to delete or retain files once their retention limit has been reached.<br><br>The auditor will examine disaster recovery in detail in Audit 69180/001, and will review data retention in back-ups as part of that audit, as the Authority is changing its DR arrangements. | Data are retained for longer than permitted by the Data Protection Act 1998, leading to the imposition of fines or other penalties by the ICO. |

### 3.1 Original Agreed Actions

We will introduce named Information Asset Owners (IAOs) with primary responsibility for ensuring record management policies are implemented and adhered to.

We will provide support to IAOs through the work of the Records and Information Manager migrating data and records into the HUB.

## 3.2 Current Position

A new information management strategy has been created and agreed by both members and management team (July 2015). This includes agreement for the creation of IAO's across the organisation. The implementation is being delayed as the organisation is undergoing a restructure and so it would not make sense to position IAOs now as their spread across the organisation would change over this year as a result of that restructure.

## 3.3 Agreed Actions

Named IAOs to be introduced.

| | |
|---|---|
| **Priority** | 3 |
| **Responsible Officer** | Head of Information Management |
| **Timescale** | 31st December 2016 |

## 4 Information asset register

| 4 Original Findings | Original Risk |
|---|---|
| The Authority does not have an information asset register. The Retention Policy is the closest equivalent, as it breaks down data held by organisation area, but may not be complete. There is no definitive central record of all data held, in which the Authority assesses the purpose and significance of the data which it holds, and the risks associated with them, and assigns responsibility for them to individual asset owners. | Data processing breaches the Data Protection Act 1998, leading to the imposition of fines by the ICO. |

### 4.1 Original Agreed Actions

We accept there is no definitive central record of all data. Information is registered in certain areas (e.g. Planning and A-Files) but elsewhere teams and individuals store data according to their needs. This situation will change with the introduction of the HUB. Business data and records will be cleansed and migrated from heritage systems into HUB where indexed meta data will be used to create and maintain an information asset register. The records and information manager will work with IAOs to support this process and, together with other staff, work to cleanse any other data to ensure it meets the standards set out in the information management policies framework.

### 4.2 Current Position

The HUB has now been developed and currently contains references to 55 categories of data (such as planning applications, or listed building, or conservation areas etc.). As part of the current approved information management strategy, work will continue as a business as usual activity to cleanse further categories of data and to introduce consistent methods of management for those data sets. There is no end date for this activity, as the data that the organisation uses is constantly growing and changing, and so this action ongoing.

The implementation of IAO's was delayed due to an organisational restructure. This will now take place from September 2016 when the organisational changes are due to be agreed and implementation started. Although the IAO's will provide a formal management structure for data management across the organisation, this ongoing activity to migrate and cleanse data need not be impacted as it is being built into specific projects anyway.

### 4.3 Agreed Actions

No further action required.

## 5 Storage and destruction of confidential information

| 5 Original Findings | Original Risk |
|---|---|
| The Information Management Policies Framework states "if the personal or sensitive data is on paper, card or microfiche, it should be destroyed mechanically using bulk shredding (available through HR or Property Services)". The auditor observed the confidential waste receptacle in HR - this was a sack, rather than a locked bin. The sacks are left open while in the building, but the auditor was informed that they are secured when removed from the building.<br><br>The auditor was informed that the HR office is kept locked when it is unoccupied and that the cleaners do not have keys. However, the Safety Officer is also a member of the HR team, and has access to the office, as does the Property Service.<br><br>Elsewhere there are no secure arrangements for holding confidential information prior to destruction - this could be commercially sensitive information, not necessarily personal data covered by the DPA. | Access to personal or commercially sensitive data by unauthorised persons (including other members of PDNPA staff), leading to imposition of financial penalties by the ICO, and/or reputational damage. |

### 5.1 Original Agreed Actions

Secure storage bins for sensitive documents to be installed around the building.

Provide lockable cabinets to those areas where sensitive/confidential information is held.

### 5.2 Current Position

Secure waste bins have been installed. Lockable storage is now available where appropriate.

### 5.3 Agreed Actions

No further action required.

## 6 Procedures for responding to an information security breach

| 6 Original Findings | Original Risk |
|---|---|
| The Authority does not have any documented policy or procedure for handling a data security breach. The Head of Information Management and the Records and Information Manager advised that they would use the information resources on the ICO website to decide how to deal with a breach. | Failure to improve procedures, leading to the imposition of fines by the ICO. |

### 6.1 Original Agreed Actions

Amendments made to the Information Management Policies Framework, setting out procedure for suspected or actual security breaches. Staff informed by email.

### 6.2 Current Position

As well as an update to the information management policies, the records and information manager makes use of the resources supplied by the ICO, including their guidance on data security breach management. We will incorporate revisions from the General Data Protection Regulation into our policies and guidance for staff, once the text of the GDPR has been agreed.

### 6.3 Agreed Actions

No further action currently necessary.

## 7 Review of Information Management Policies Framework

| 7 Original Findings | Original Risk |
|---|---|
| The Framework has a version history, but there is no review interval indicated, and it does not formally assign responsibility for reviews. | The Authority does not respond to changes in legal requirements relating to information governance. |

### 7.1 Original Agreed Actions

Updates to policies to be made as required with staff informed. (Example Procedure for security breach, item 6 above.). Complete review of framework every two years.

### 7.2 Current Position

A review schedule has been added to the information management policies framework with a full review scheduled every two years.

### 7.3 Agreed Actions

No further action required.

# Audit Opinions and Priorities for Actions

| Audit Opinions | |
|---|---|
| Audit work is based on sampling transactions to test the operation of systems. It cannot guarantee the elimination of fraud or error. Our opinion is based on the risks we identify at the time of the audit.<br>Our overall audit opinion is based on five grades of opinion, as set out below. | |
| **Opinion** | **Assessment of internal control** |
| High Assurance | Overall, very good management of risk. An effective control environment appears to be in operation. |
| Substantial Assurance | Overall, good management of risk with few weaknesses identified. An effective control environment is in operation but there is scope for further improvement in the areas identified. |
| Reasonable Assurance | Overall, satisfactory management of risk with a number of weaknesses identified. An acceptable control environment is in operation but there are a number of improvements that could be made. |
| Limited Assurance | Overall, poor management of risk with significant control weaknesses in key areas and major improvements required before an effective control environment will be in operation. |
| No Assurance | Overall, there is a fundamental failure in control and risks are not being effectively managed. A number of key areas require substantial improvement to protect the system from error and abuse. |

| Priorities for Actions | |
|---|---|
| Priority 1 | A fundamental system weakness, which presents unacceptable risk to the system objectives and requires urgent attention by management. |
| Priority 2 | A significant system weakness, whose impact or frequency presents risks to the system objectives, which needs to be addressed by management. |
| Priority 3 | The system objectives are not exposed to significant risk, but the issue merits attention by management. |



PEAK DISTRICT NATIONAL PARK

Where information resulting from audit work is made public or is provided to a third party by the client or by Veritau then this must be done on the understanding that any third party will rely on the information at its own risk. Veritau will not owe a duty of care or assume any responsibility towards anyone other than the client in relation to the information supplied. Equally, no third party may assert any rights or bring any claims against Veritau in connection with the information. Where information is provided to a named third party, the third party will keep the information confidential.