Information Governance

Peak District National Park Authority

Internal Audit Report 2020-21

Business Unit: Corporate
Responsible Officer: IT Manager
Service Manager: Records and Information Manager (DPO)
Date Issued: 1 March 2021
Status: Final
Reference: 69140/009

	P1	P2	P3
Actions	**0**	**0**	**0**
Overall Audit Opinion	Substantial Assurance		

Summary and Overall Conclusions

Introduction

The General Data Protection Regulation (GDPR) and Data Protection Act were introduced in May 2018. GDPR changed the data processing requirements for organisations. These changes include a strengthening of the conditions for consent, greater rights for data subjects, the requirement for privacy by design, greater enforcement powers, and an increase in the maximum potential fine to €20 million or 4% of annual global turnover (whichever is greater).

The Peak District National Park Authority (PDNPA) processes the following types of personal data: information on applicants for posts; employee and volunteer information; member contact details; and service user information. Overall responsibility for personal data processed lies with the Leadership Team, who delegate tasks to the Data Protection Officer (DPO). The last audit covering Information Governance took place in 2018-19 and was given a Substantial Assurance rating.

Due to the Covid-19 outbreak in spring 2020, there has been a significant increase in PDNPA employees working remotely from home. It is essential effective controls are in place with regards to information governance during this period to provide oversight and assurance over the use of personal data.

Objectives and Scope of the Audit

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

- Appropriate policies and procedures were in place and were compliant with GDPR requirements.
- Staff were provided with guidance on compliance with GDPR.
- Records were kept of Subject Access Requests and Freedom of Information Requests.

Policies, procedures, and guidance provided to staff were reviewed to check that they were appropriate for home working.

Key Findings

We found that the Authority had appropriate policies and procedures in place. The Authority's main document for data protection is the Data Protection Policy. An effective data protection policy should set out data protection requirements under GDPR, provide guidance on data protection to operational staff, and outline roles and responsibilities for data protection within the organisation. The PDNPA Data Protection meets all of these requirements. In addition, the policy is complemented by separate procedure guidance documents for records management, data breaches and security incidents, data protection and consent, data sharing, data protection impact assessment, subject access requests, clear desk policy, freedom of information requests, collaboration tools, and CCTV. We also saw that the Data Protection Policy had been recently reviewed in September 2020 and that an appropriate review schedule was in place.

Most policy documents are available through the Peak District's website so are available for staff to access. Guidance provided is comprehensive and additional guidance has been provided to staff since the beginning of the Covid-19 pandemic where staff have often been required to work from home. The Authority have issued Covid-specific guidance documents on using WhatsApp for work purposes and keeping Zoom meetings secure. In addition, the clear desk policy was reviewed and email reminders sent out to staff to emphasise the importance of data security when dealing with potentially sensitive documents in a home environment.

All staff are required to complete a data protection training module via the ELMS e-learning system. As of October 2020, all 259 staff on the ELMS completion report we saw had completed the training. Most staff appear to have completed the training in a timely fashion although we did identify three instances where staff had taken over 12 months to complete the training. It was explained that in the past, new staff had sometimes been missed off the ELMS system. However, a new process has been brought in whereby IT are responsible for entering new starter data onto the ELMS system which now has the capability to send automated reminder emails. Beyond this, there is a process in place to escalate non-completions if staff do not respond to the automated emails.

The Authority receive very few Subject Access Requests (SARs), two during 2020. They receive more Freedom of Information Requests, 26 in 2020. We reviewed the policies and procedures for SARs and FOIs and found both to be sufficient. There is a 'Managing a Subject Access Request' document in place that should appropriately guide staff in dealing with an SAR if followed. There is a similar document for FOIs, the 'Procedure for Dealing with FOI Requests' is in place that, similarly, should appropriately guide staff through what to do if they receive an FOI request.

An FOI and SAR Disclosure Report is created and published on the Authority's website quarterly. We reviewed the reports from July and September 2020. Seven FOI requests and no SARs were received in this period. Of the seven FOI requests, all have been appropriately responded to within the necessary timescales indicating that processes for FOI requests are working effectively in practice. The Authority also have responded appropriately and within the necessary timescales for both SARs received during 2020, again indicating that processes and procedures are working well.

Overall Conclusions

A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited. Our overall opinion of the controls within the system at the time of the audit was that they provided Substantial Assurance.

Annex 1

Audit Opinions and Priorities for Actions

Audit Opinions	
Our work is based on using a variety of audit techniques to test the operation of systems. This may include sampling and data analysis of wider populations. It cannot guarantee the elimination of fraud or error. Our opinion relates only to the objectives set out in the audit scope and is based on risks related to those objectives that we identify at the time of the audit. Our overall audit opinion is based on 4 grades of opinion, as set out below.	
Opinion	**Assessment of internal control**
Substantial Assurance	A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.
Reasonable Assurance	There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited.
Limited Assurance	Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited.
No Assurance	Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited.

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.

PEAK DISTRICT NATIONAL PARK