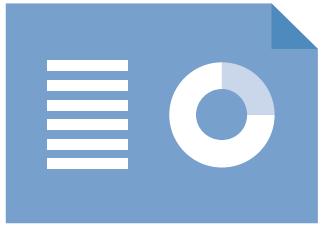
North Yorkshire Police

Data protection audit report

July 2019

Information Commissioner's Office

Executive summary



Audit Methodology

The Information Commissioner is responsible for enforcing and promoting compliance with the General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA18) and other data protection legislation. Section 146 of the DPA18 provides the Information Commissioner's Office (ICO) with the power to conduct compulsory audits through the issue of assessment notices. Section 129 of the DPA18 allows the ICO to carry out consensual audits. The ICO sees auditing as a constructive process with real benefits for controllers and so aims to establish a participative approach.

North Yorkshire Police (NYP) agreed to a consensual audit by the ICO of its processing of personal data. The on-site audit was undertaken at NYP Headquarters and Northallerton Police Station, Alverton Court, Northallerton, North Yorkshire DL6 1BF.

The purpose of the audit is to provide the Information Commissioner and NYP with an independent assurance of the extent to which NYP, within the scope of this agreed audit, is complying with data protection legislation.

It was agreed that the audit would focus on the following area(s):

Scope Area	Description
Governance & Accountability	The extent to which information governance accountability, policies and procedures, performance measurement controls, and reporting mechanisms to monitor data protection compliance to both the GDPR and national data protection legislation are in place and in operation throughout the organisation.
Data Sharing	The design and operation of controls to ensure the sharing of personal data complies with the principles of all data protection legislation
Training & Awareness	The provision and monitoring of staff data protection, records management and information security training and the awareness of data protection regulation requirements relating to their roles and responsibilities.

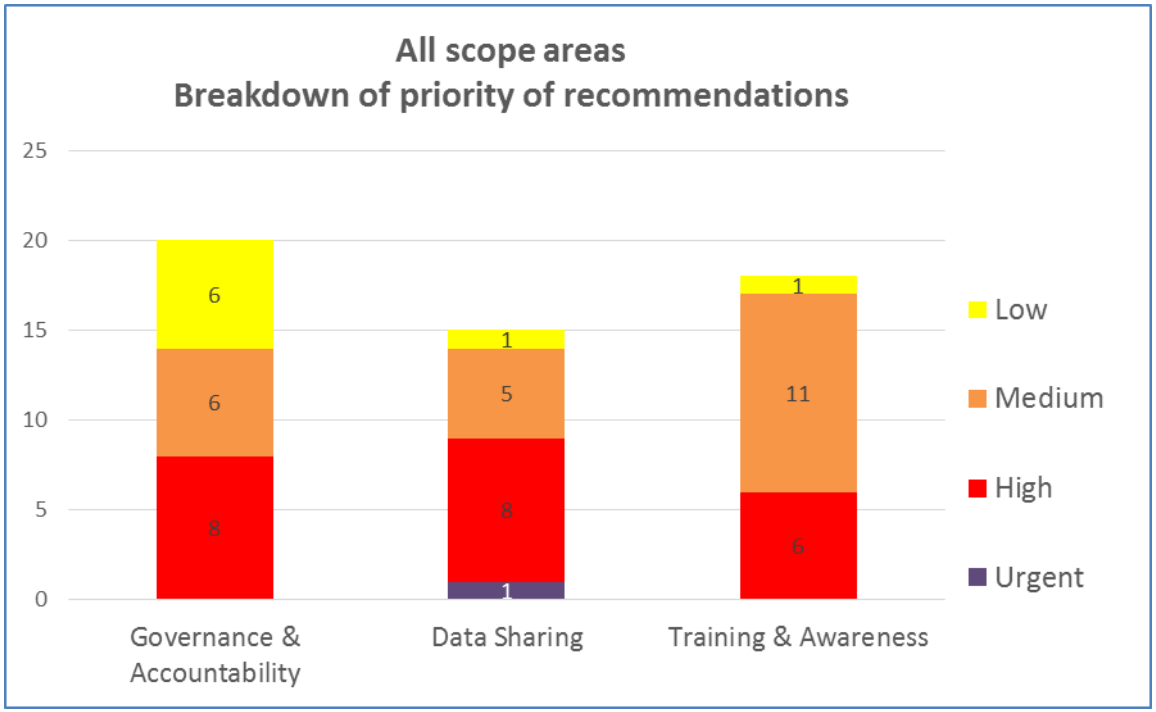
The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist NYP in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. NYP priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

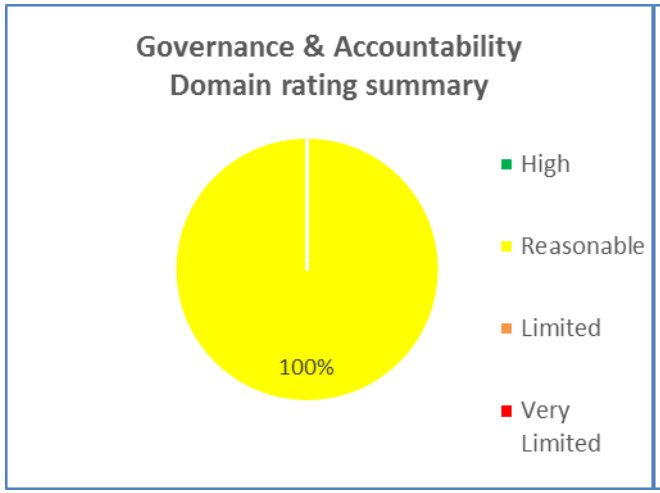
Audit Summary

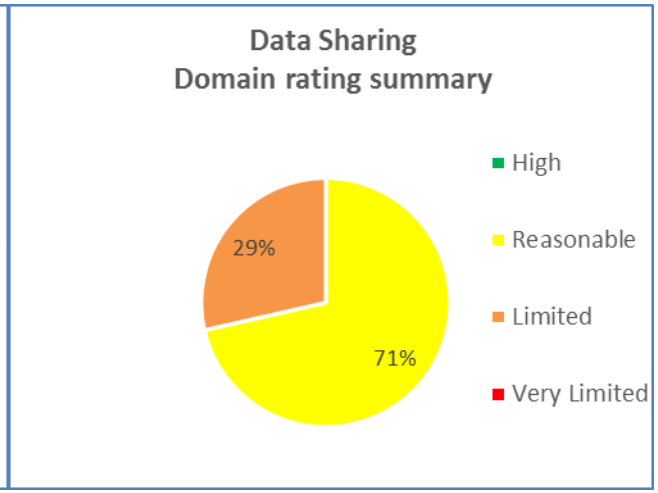
Audit Scope Area	Assurance Rating	Overall opinion
Governance & Accountability	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Data Sharing	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Training & Awareness	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.

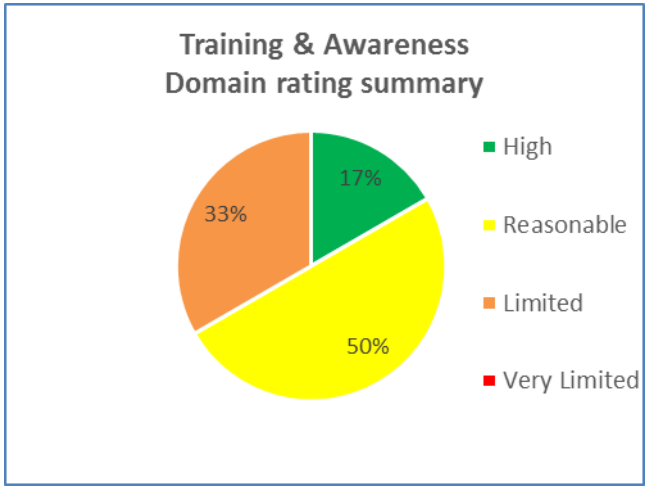
Priority Recommendations



Graphs and Charts







Areas for Improvement

There are no processes in place to gain assurance that staff have read and understood current information governance policies and procedures and are aware of their responsibilities.

NYP do not have a formal data protection/information governance audit plan and there are no scheduled spot checks undertaken to identify issues and to provide assurance that policies and procedures are being followed

There are no reviews of consent mechanisms used across the force to ensure that sufficient information is being provided to individuals giving consent, and there are no processes in place to consider refreshing these consents.

A Data Protection Impact Assessment (DPIA) procedure is in place but this needs to be embedded into their local procurement policies and procedures, this will ensure that DPIA completion takes place whenever they are considering any high risk data processing activities.

The creation of the new Information Asset Register/Record of Processing has identified a large number of information sharing activities that are not supported by formal agreements. There is also a backlog of existing information sharing agreements that have not been updated with GDPR/DPA 18 requirements and/or are overdue their scheduled review.

There is a national problem with retention and disposal of information on the Niche system. NYP do not undertake spot checks to ensure that only data within its retention period is being shared.

An overall training programme and delivery plan for information governance is required that captures both national provision from the College of Policing and additional needs based training identified for all staff. Steps should be taken to ensure the training is effective with a mixture of face-to-face classes and online learning.

Training provision should be overseen by the Information Management department to gain assurance that content is accurate and up-to-date with current data protection legislation. In addition, the training completion rates

should be monitored using agreed KPIs so that compliance can be reliably monitored by senior management.

Good Practice

NYP have developed a regimented and consistent communication system for updating staff on information governance. Led by the DPO they use the intranet to circulate a mixture of learning bulletins, new messages, policies/procedures and trends in data breaches. Information bulletins have been targeted at those involved with non-compliance. Maintaining a high profile information governance campaign has further elevated the importance of data protection compliance across the organisation.

Disclaimer

The matters arising in this report are only those that came to our attention during the course of the audit and are not necessarily a comprehensive statement of all the areas requiring improvement.

The responsibility for ensuring that there are adequate risk management, governance and internal control arrangements in place rest with the management of North Yorkshire Police.

We take all reasonable care to ensure that our audit report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however such loss or damage is caused. We cannot accept liability for loss occasioned to any person or organisation, including any third party, acting or refraining from acting as a result of any information contained in this report.

This report is an exception report and is solely for the use of North Yorkshire Police. The scope areas and controls covered by the audit have been tailored to North Yorkshire Police and, as a result, the audit report is not intended to be used in comparison with other ICO audit reports.