REPORT TO:	**STRATEGIC SCRUTINY MEETING**
DATE:	**September 2020**
TITLE:	**Information Governance Annual Report 2019/20**
REPORT BY:	**Carl Melling**

1. Issue for Consideration

The purpose of this report is to provide the Commissioner with an overview of the Constabulary's performance and progress in relation to information governance during 2019/20.

2. Recommendation

The Commissioner is requested to review the report and make comments as appropriate.

3. Background

The Constabulary's Information Governance Board, chaired by the Director of Resources who is the Senior Information Risk Owner (SIRO), oversees and considers Information Governance issues for Lancashire Constabulary.

The Board provides the high-level oversight, strategic direction, and leadership within the Force seeking to maximise the benefits of operational information in order to support effective decision making and to ensure the safe and lawful use of police information.

The Board oversees Force compliance with its statutory obligations, including those arising from the General Data Protection Regulation, Data Protection Act 2018, Freedom of Information Act 2000 and compliance with such as the Management of Police Information (MOPI) guidance and NPCC Community Security Policy.

Whilst the outcome of the organisational review, which has created the Data Protection Office as a standalone Department with effect from April 2020, will enhance the ability of the Chief Constable to meet his statutory obligations more effectively and efficiently, the period of transition has been challenging.

The increase in demands that were anticipated as a consequence of the new data protection legislation in 2018 has materialised including; greater volumes of requests for information, increased reports of security incidents, requests for support and advice for corporate digital projects, as required by the need to implement data protection design and default plus undertaking data protection impact assessments.

The above is in the context of significant staff turnover leading to continued vacant posts and more latterly the impact of the Covid-19.

The establishment of the Data Protection Department, recognises the statutory requirement for the Data Protection Officer to be independent, suitably positioned and resourced to carry out their statutory tasks. The Department is comprised of Information Security, Records Management, Information Access (data protection and freedom of information), and Data Protection Compliance and Audit.

The separation from the (family court and civil) Disclosures Team which remains, along with the Disclosure and Barring Service Team, within Legal Services thereby provides a structure in which information governance functions are aligned and free from dilution from its core purpose.

The clear department identity will assist colleagues and members of the public and facilitate a more efficient service enabling enquiries to be directed more effectively; and providing one measure which enables the Chief Constable to demonstrate compliance with the statutory requirement relating to the data protection principle of accountability.

The establishment of a resource to deliver an effective information management audit programme supporting each function will help identify data quality issues and help raise awareness of risks with Information Asset Owners (IAOs), under the oversight of the Information Governance Board.

The alignment of the triumvirate of information governance functions will assist in developing and retaining knowledge and enhance resilience. The loss of and ability to attract data protection/ information security specialists is recognised as a risk by the National Police Chiefs Council (NPCC). Whilst a relatively small department its establishment does provides a clear career pathway in which staff can develop within the Force in this specialised area.

This report provides a summary of performance and issues during the period 2019-2020.

4. DATA PROTECTION COMPLIANCE AND ICO AUDIT

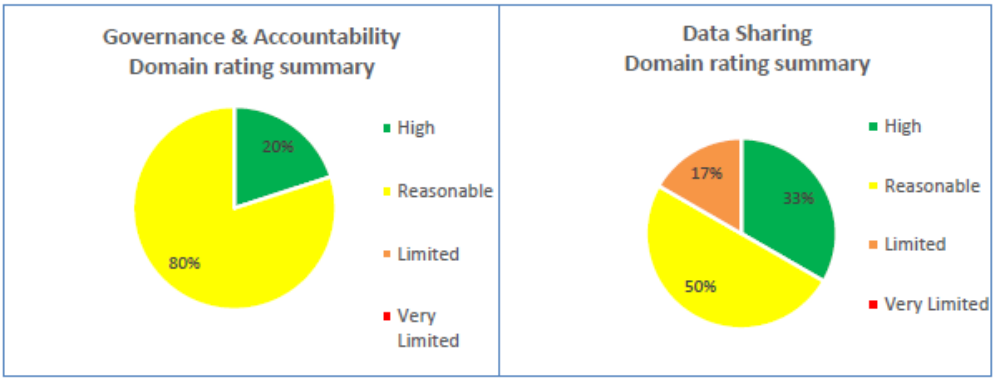
In April 2019, the Information Commissioner undertook a consensual data protection audit of Lancashire Constabulary.

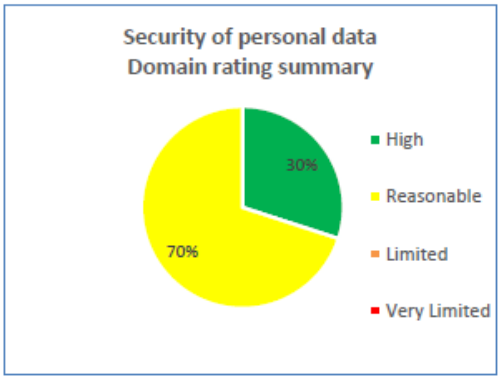
The audit Report was received in June 2019. The audit focussed on

Governance and Accountability, Data Sharing and Information Security.

The assurance rating received for each area in scope was “Reasonable”, broken down as follows:

Graphs and Charts





The report contained 67 recommendations, four of which were classified as Urgent. Of the 67 recommendations, 49 were accepted, 12 were partially accepted and 6 were rejected.

During 2019/20, and working with colleagues in Information and Communications Technology (ICT), progress has continued to be made to address the recommendations, in particular those that were identified as urgent or high priority. A number of recommendations related to compliance issues that had already been identified and which could be addressed once the data protection office was established and up to establishment.

With regard to the ‘Urgent’ recommendations that were accepted progress continues to be made to complete the Record of Processing Activities (a statutory requirement) and to document the lawful basis for processing**.** Records of data flows from most departments are now documented (75%). It continues to be the main priority for the Data Protection Auditor in post (the other post remaining vacant for some time).

A revised Force General Privacy Notice was published on the Force website in

March 2020, together with a Child Friendly Privacy Notice. A template Privacy Notice for 'specific' processing has been established which was circulated to all Information Asset Owners for completion as necessary.

The Data Protection Officer now reports directly to the Senior Information Risk Owner (SIRO) meaning that appropriate reporting mechanisms are in place. Additional vulnerability and PEN testing have been added to internal ICT auditing procedures which are to be conducted on a quarterly basis. A number of policies have been updated such as the Data Protection Policy, Information Security, Acceptable Use and Remote Working Policies, to reflect the provisions of the GDPR and the DPA18. Information Asset Owner bulletins and updates have been issued periodically.

Awareness of the requirement to complete Data Protection Impact Assessments (DPIA) prior to any new initiative/ system being commissioned/ commencing is now largely understood within the Force and a number of DPIAs have been completed during the period. Once completed there is a requirement to monitor, review and update.

However, further work is required to address other recommendations contained within the ICO Report relating to the development of training and communication, finalisation of the ROPA, implementation of programme compliance audit of work and security spot checks, reviewing new and existing training materials for accuracy, and reviewing and updating information sharing agreements.

5. INFORMATION ACCESS REQUESTS: PERFORMANCE

During 2019 and following engagement with the NPCC the Information Commissioner commenced a monitoring exercise relating to the performance of all Forces with regards to compliance with the statutory timescales set out within data protection and freedom of information legislation. Whilst this had been an area of weakness for a period, due to the resource issues and growth in demands, performance had improved by the time they ICO commenced monitoring.

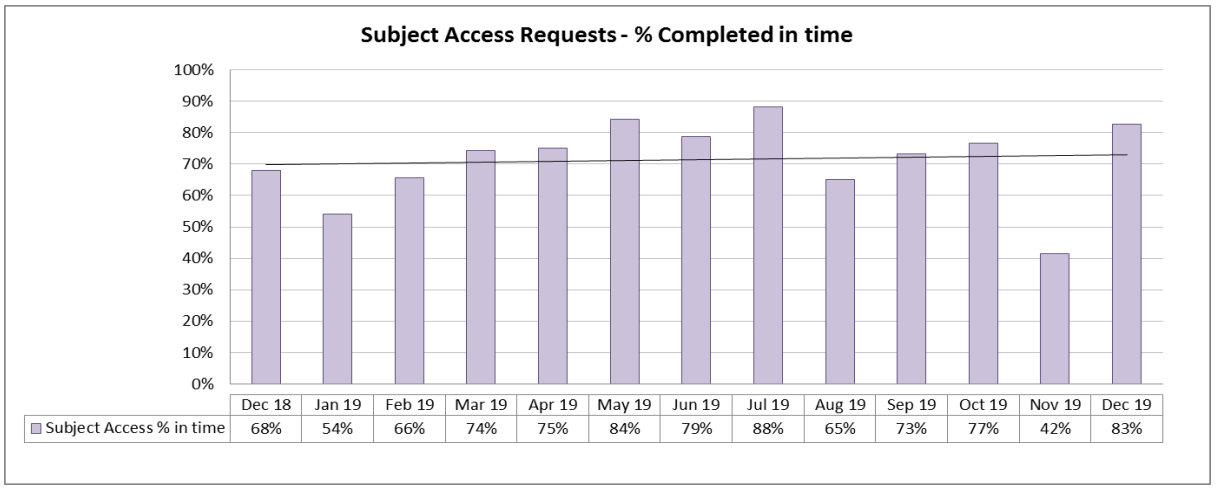
Subject Access

In the 2017 calendar year, prior to the introduction of the new data protection legislation being introduced 398 subject access requests were received from individuals seeking access to their personal data held by Lancashire Constabulary.

In 2019, 632 subject access requests were received (61% increase).

The ICO has previously indicated that they expect organisations to be compliant with statutory timescales in 90% of the requests received.

Compliance Rates:	2018	68%.
	2019	72%
(Jan – Mar)	2020	88%



Of particular note during the period is the volume of requests for digital information, eg body worn video which can be particularly time burdensome and time consuming.

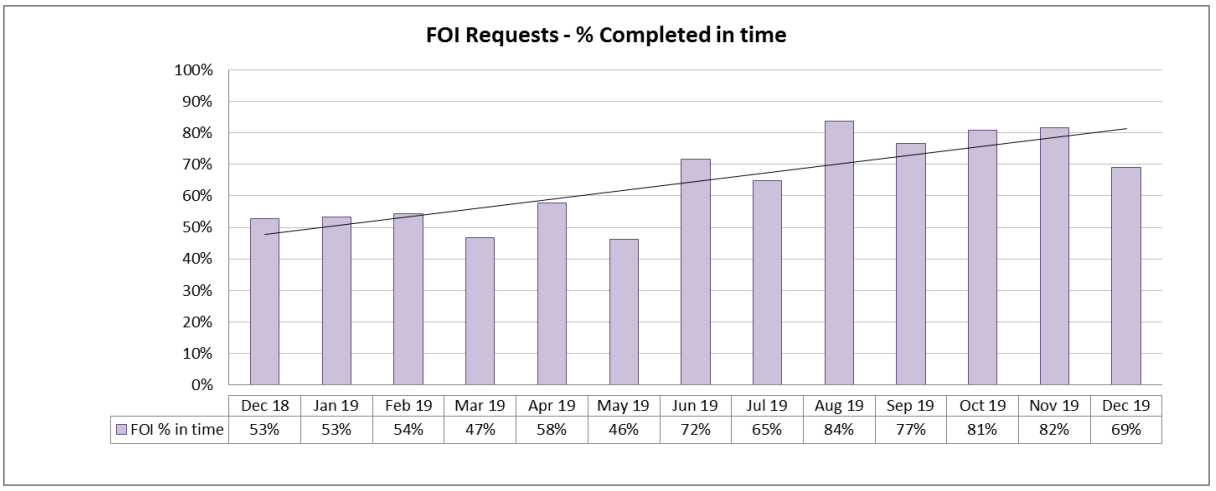
Complaints:

In 2019/20 18 internal review requests were received and 11 complaints were made to the Information Commissioner in comparison with 8 complaints made to the Information Commissioner in 2018/19.

Freedom of Information (FOI)

The number of FOI requests received in 2019/20 was 1347, which is a small increase in the number received in 2018/19.

Compliance Rates:	2018	57%
	2019	66%
(Jan – Mar)	2020	84%



	Dec 18	Jan 19	Feb 19	Mar 19	Apr 19	May 19	Jun 19	Jul 19	Aug 19	Sep 19	Oct 19	Nov 19	Dec 19
FOI % in time	53%	53%	54%	47%	58%	46%	72%	65%	84%	77%	81%	82%	69%

Internal Reviews (complaints) received: 2018 43
2019 57

Three complaints were made to the ICO.

6. MANAGEMENT OF POLICE INFORMATION (MoPI)

The Data Protection Act 2018 requires that personal data processed for law enforcement purposes must not be kept for longer than necessary and reviewed in accordance with specified time limits.

MoPI sets out the guidance relating to the appropriate time periods to review/ retain police record relating to individuals. The Force has been moving towards compliance with MoPI during its implementation of the CONNECT system.

National work has also been on-going to review the national MoPI guidance and to identify whether some records might be suitable for automated deletion. However, once back record conversion of historic records from Sleuth/ legacy systems has been completed it is highly likely that manual intervention will be required to review those records that are flagged for review. In due course consideration will need to be given to the Force policy to be adopted applied relating to the review and retention of records in line with MoPI, this may require growth in the Records, Review and Deletion Team (RRD), which presently comprises of four posts.

In the meantime, during 2019/20 the RRD Team reviewed and amended intel records of 2000 nominals and undertook 4,000 scheduled reviews, whereby 1000 nominal records were identified for potential deletion. 28 applications from subjects requesting deletion from PNC were received of which 27 were approved.

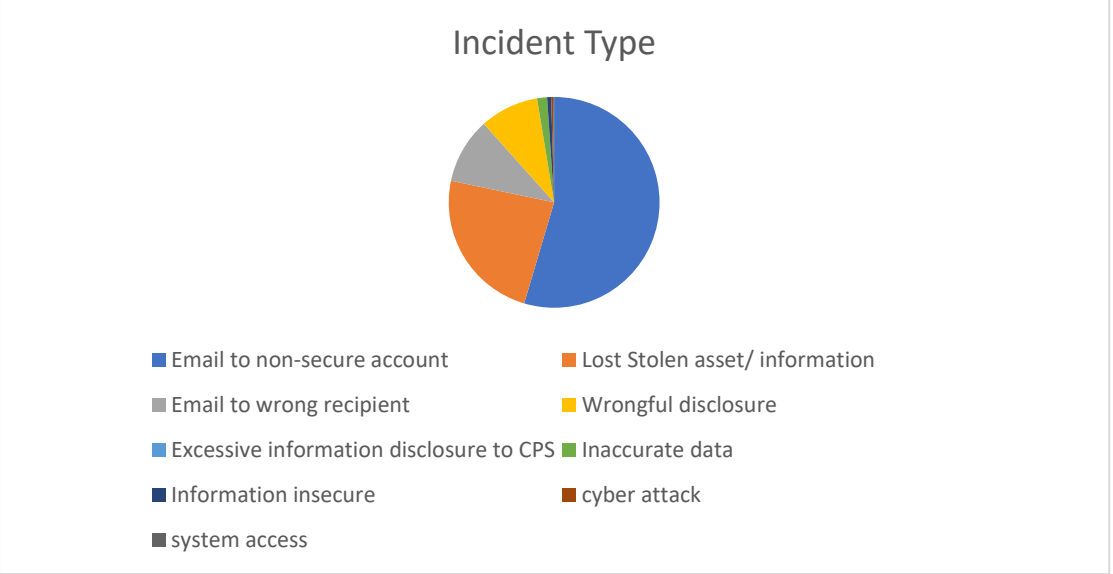
7. INFORMATION SECURITY

As with all large organisations' security incidents[1] occur and are managed with rigour. Any incident or security breach is analysed and processes and policies continue to evolve so as to reduce any future exposure and repetition.

The promotion and communications concerning the requirement to report incidents and potential personal data breaches, so as to enable potential notification to the Information Commissioner in accordance with statutory requirements has seen an increase in the number of incidents reported in 2019/20.

2018 Incidents Reported	346
2019 Incidents Reported	460 (+33%)

The monthly average of reported incidents prior to the implementation of the Data Protection Act 2018 was 21. The monthly average of incidents reported in 2019 was 38. A breakdown of incident types is set out below.



In 2019 three incidents were referred to the Information Commissioner. Two resulted in no further action. One remains the subject of an on-going investigation; this was the incident which affected the whole of the police service arising from the ransomware attack on Eurofins.

[1] A security incident involves the actual loss, (or near miss), of personal or classified information assessed to present harm to an individual, a system, or the organisation

8. DISCLOSURES (Family Proceedings)

2019/20 saw a considerable increase in requests for disclosure for police information in relation to family proceedings, 1368 compared to 1131 in 2018/19 (+21%). In part this is because local authorities sought to deal with more cases at the pre-proceedings stage. Due the various risks arising from failing to meet deadlines, support was provided to the Team to cover vacancies etc from other areas of the "data protection office".

A detailed submission was made, on behalf of the NPCC, to the family justice review highlighting the difficulties being encountered across the service in meeting the ever growing and burdensome disclosure demands and suggesting that national protocols should be reviewed. Lancashire seeks to recover costs for disclosure. Representations have also been made, on behalf of the NPCC, to the Ministry of Justice regarding the need to consider the cost burden to forces within any future national guidelines.

9. PRIORITIES FOR 2020/2021

The key priority, which impacts on all the departmental objectives, is to ensure that the Data Protection Office is operational at or close to full establishment as soon as possible; this has not been possible over the past few years mainly due to the temporary nature of a number of posts, which causes issues with staff retention. The permanent new structure will assist in mitigating this risk, albeit this may be challenged by the risk of further resource cuts over the CSR period. In particular as the further engagement planned will likely result in an increase in the demand for the services of the department.

In 2020 an audit of Force training materials will be undertaken to ensure GDPR/ DPA 2018 compliance and to verify that the content of the training correctly reflects data protection and is up to date. The immediate focus within the audit programme remains completion of the information audit to inform the Record of Processing Activities but as soon as resources allow a risk-based audit programme will commence. It is also planned to promote greater awareness of the risks of poor information management through our internal media campaign.

Support will continue to be provided to the implementation of national and local projects (NEP/ O365/ DEMS) whilst maintaining national security accreditation certificates, enhancement of the Departmental Training and Engagement Plan. Other priorities will be to develop further management information which will inform the Information Management Risk Register, improve information access performance, development of staff within Department, and to deliver the DPO services to the OPCC.