For Information	
Public/Non Public*	**Public**
Report to:	**Strategic Resources and Performance Meeting**
Date of Meeting:	**29th March 2018**
Report of:	**Deputy Chief Constable as Senior Information Risk Owner**
Report Author:	**Pat Stocker – Information Management Lead**
E-mail:	**pat.stocker@nottinghamshire.pnn.police.uk**
Other Contacts:	
Agenda Item:	**8**

*If Non Public, please state under which category number from the guidance in the space provided.

Information Management Update March 2018

1. Purpose of the Report

1.1 The purpose of the report is to inform the Strategic Resources and Performance Meeting on the current position of the functional areas within Information Management including:

- Data Protection, Information Sharing and Compliance Audit including GDPR
- Disclosure including Freedom of Information (FOI) and Data Protection requests
- Information Security & Information Asset Management and Risk Management
- Records Management

1.2 Information Management performance is monitored and reported to the Force Information Management Board chaired by the Deputy Chief Constable.

2. Recommendations

2.1 The Police and Crime Commissioner is asked to note the contents of this paper and advise on the frequency and content of future Information Management reports

3. Reasons for Recommendations

3.1 This is the first report of its type to be requested by the Police and Crime Commissioner.

4. Summary of Key Points

DATA PROTECTION

General Data Protection Regulations (GDPR) and Data Protection Bill 2017

- Comes into force on 25th May 2018.
- Many areas are similar to the current Data Protection Act 1998. Please see Appendix A, which highlights what is new.

Actions:

- A working group has been formed consisting of the Information Management (IM) Lead and IM Team Leaders. This is in the process of completing a series of self-assessment gap analysis documents provided by the National Data Protection Reform Group to assess our current compliance level.

- Once the gap analysis has been completed priority areas will be identified and an implementation plan prepared for agreement and monitoring at the Force Information Management Board.

INFORMATION SHARING

Nottinghamshire Police shares information for many reasons, with other forces, partner agencies and the public. Sharing information allows us to deliver a better and more effective service. It is the policy of Nottinghamshire Police to generally share information or intelligence with other third parties as long as a lawful basis can been established, except in circumstances where disclosure may compromise any Police operation, investigations and initiatives, or has the potential to cause harm to an individual.

A review of the current Information Sharing Agreements (ISA) and Data Processing Agreements (DPAs) has identified the following:

- We have 114 active ISAs
- 45 ISAs are due for review (last reviewed 2015 and prior)
- 9 new ISAs set up since September 2017
- 6 new ISAs currently under development
- 77 DPAs on file, of which only 8 are live
- All 8 DPAs are overdue for review (last reviewed 2015 and prior)
- 1 new DPA currently under development

A review of all Information Sharing Agreements and Data Processing Agreements will be required as part of GDPR implementation.

COMPLIANCE AUDIT

AUDIT SCHEDULE 2017/18: An Information Management Audit Schedule has been produced and signed off by the Deputy Chief Constable in her role as Senior Information Risk Owner (SIRO). The main purpose of this audit function is to provide the organisation with an independent assessment and appraisal of compliance with the current Data Protection Act 1998 and in the future, with the upcoming GDPR requirements.

Part one includes system audits mandated/advised for audit by Code of Connection/Memorandum of Understanding.

Part two includes business areas that have been included as the ‘core’ areas for audit are the areas originally identified in the Management of Police Information (MOPI) Guidance as being the most significant for policing purposes. Seven areas for audit have been identified including areas such as Empowering Communities Including Neighbourhoods (ECINS), Multi Agency Safeguarding Hub, Sexual Exploitation Investigation Unit, Missing Persons, Recording of Safeguarding issue, National

Firearms Licensing Management System and Violent Including Sexual Offenders Register.

Audit Schedule updates are monitored and reported to the Force Information Management Board.

DISCLOSURE – FOI AND DATA PROTECTION INFORMATION REQUESTS

Introduction and Background:

- The Disclosure team manages both FOI and subject access requests and is a small team that comprised of a Senior Officer and 2 x Disclosure Officers following the restructure of May 2016.
- Since the restructure the team has taken on the safeguarding disclosure process that used to be managed in the MASH unit including 2 dedicated resources managing these requests from relevant Local Authority Children's services.
- A consistent increase in both the numbers and complexity of the types of FOI and Data Protection requests received alongside changes in resources has resulted in significant delays in legislative compliance for FOI and DP information requests leading to an increase in the number of complaints from individuals to both the PCC's office, the Information Commissioner's Office and through the Force complaints process in the first part of 2018.
- This risk has been identified on the Corporate Development risk register and the Head of Corporate Development is aware. Overtime has been worked by Information Management Team members, when available, to assist in mitigating this risk but there is a steady flow of requests each day and only priority and urgent requests are able to be cleared down consistently.
- The Information Management function is due to be reviewed as part of the force wide restructure in the near future and it is hoped that as part of the IM review the use of Process Evolution software can be used to identify areas to improve efficiency in our processes and identify the correct level of resourcing required both now and to meet the new legislative requirements of GDPR for dealing with data subject requests.

INFORMATION SECURITY

NATIONAL POLICE GOVERNANCE AND INFORMATION RISK RETURN (GIRR)

The Governance and Information Risk Return (GIRR) has replaced previous national police reporting regimes including the Community Code of Connection and the Police Service Risk Management Overview (Information Assurance Maturity Model and Security Policy Framework) with a single annual return, reducing cost and complexity. The GIRR process is managed by the National Police Information Risk Management Team based in the Home Office.

This is aligned to the Her Majesty's Government approach of central assessment of submissions based on self-assessment with centrally conducted audits. Relevant international standards from the ISO 27000 series have been considered and applied in the development of appropriate controls based on an interpretation of these standards for policing following a risk assessment.

The purpose of the GIRR is to provide assurance and confidence that information shared between the national policing community of trust is managed appropriately and that each organisation sharing information utilises similarly appropriate information risk management regimes. The GIRR sets out the standard which any organisation wishing to connect to the national policing community of trust must meet, and ensures provision of a level of consistency within the national policing community of trust. This return must be completed and submitted on an annual basis.

Nottinghamshire Police submitted their GIRR to the National Police Information Risk Management Team (NPIRMT) in December 2017 and it is currently being processed.

PUBLIC SERVICES NETWORK

The PSN (Public Services Network) is a network operated by several suppliers for government that provides a trusted, reliable, cost-effective solution to departments, agencies, local authorities and other bodies that work in the public sector, which need to share information between themselves. The PSN process is managed by the Government Digital Services (GDS) based in the Cabinet Office.

This document is completed by any organisation wishing to connect to the PSN. It outlines conditions that need to be met and the information that is required to be provided. This information will be used to assess whether an organisation may connect/continue to connect to PSN. The PSN team may also need to conduct an on-site assessment. A PSN connection compliance certificate is required prior to connection to the PSN.

Nottinghamshire Police are in the process of completing their PSN assessment prior to submission.

SECURITY INCIDENT REPORTING AND DATA BREACHES

Quarterly reporting of security incidents is mandated on all Police Forces by the National Police Information Risk Management Team (NPIRMT). There is also a requirement to self-report any relevant data breaches to the ICO as per the link below: https://ico.org.uk/media/for-organisations/documents/1536/breach_reporting.pdf

National reporting for information security incidents is divided into two processes.

Slow time incidents: involving the actual loss, (or near miss), of personal or classified information assessed to present limited harm to individuals or the force, are local in nature, and have no characteristics that require the rest of the community to be immediately notified. This guidance is intended for slow time incidents.

Reporting is done by providing NPIRMT (National Police Information Risk Management Team) of incidents on a quarterly basis.

Fast time incidents: involving the actual loss of personal information that could cause significant harm to individuals or compromise systems that could potentially effect national systems/connectivity.

Reporting incidents irrespective of what media is involved and includes both electronic and paper records. Forces have a national requirement, to report information security incidents and provide quarterly returns to the Police Information Assurance Board (PIAB).

Nottinghamshire Police submitted their Quarter 4 return to NPIRMT in January 2018 and identified 16 slow time incidents, 2 of which were near misses.

There have been no self-referrals to the ICO during 2017.

INFORMATION ASSET MANAGEMENT

The Master Information Asset Register (IAR) was initially created in 2014 and was further developed in 2016 following the Force re-structure.

Further development of the register has been delayed due to the recruitment process for the Information Security Officer in 2017 and the imminent Force re-structure due in April 2018.

Part of the GDPR implementation plan will identify the importance of completing a Data Flow mapping exercise to identify personal and sensitive data processed by the Force, the relevant Information Asset Owner (IAO) of that data and the responsibilities of the IAO for that data.

CORPORATE RISK MANAGEMENT INCLUDING INFORMATION RISK

The aim of the Corporate Risk Management Strategy is to establish and embed within normal business practice and culture, the foundations for efficient and effective corporate risk management to predict and prepare for future challenges and support Nottinghamshire Police and NOPCC in the achievement of their objectives.

The strategy will be used to manage all types of risk including corporate, operational, financial and information risk, in a simple, robust and standardised approach.

The Corporate Risk Management Process is still under development and is being monitored by the Deputy Chief Constable and update reports provided as necessary.

RECORDS MANAGEMENT

The Records Management Officer post within the Information Management Team was identified in the Information Management restructure of 2016 and recruited to in July 2017 as a result of issues relating to:

- Review, Retention and Disposal (RRD) processes including the implementation of the Regional RRD Team connected to Niche and led by Lincolnshire Police. The implementation date for the Regional RRD process is due to be some time in March 2018.

- IICSA / UCPI – National Inquiries that both have a requirement to review historical data both electronic and hard copy.
- Hard Copy Records - to review the processes surrounding hard copy records currently stored within the Force Estate or retrieved from recently closed premises in line with the National Retention Schedule (Links to GDPR Data Flow Mapping requirement).
- Iron Mountain – to review the current processes for off-site storage provided by the current external provider to ensure it remains value for money and fit for purpose.

Nottinghamshire Police are in the process of reviewing all processes and policies connected with Records Management to ensure that relevant risks and issues are identified and managed according to priority and risk assessment.

5. Financial Implications and Budget Provision

5.1 Any financial implications identified as part of the Information Management and GDPR review will be progressed through the Force Business Change process

6. Human Resources Implications

6.1 There are no additional HR implications other than those identified in the main body of this report.

7. Equality Implications

7.1 There are no equality implications arising from this report.

8. Risk Management

8.1 Any risks identified through the Information Management and GDPR review process will be progressed through the Force Corporate Risk process

9. Policy Implications and links to the Police and Crime Plan Priorities

9.1 Good Information Management will support the delivery of both the Chief Constables and PCC's priorities by providing:

- Good quality data, accurate & up to date and available when required
- Collected and shared where appropriate and kept for only as long as necessary
- Knowing what we have and where it is will make us more effective and efficient

10. Changes in Legislation or other Legal Considerations

10.1 New Data Protection Legislation – GDPR and Data Protection Act 2017 become enforceable on May 25th 2018.

11. Details of outcome of consultation

11.1 No consultation took place in the production of this report.

12. Appendices

12.1 Appendix A – GDPR, ‘What’s New?’ document: