For Information	
Public/Non Public*	Public
Report to:	Strategic Resources and Performance Meeting
Date of Meeting:	24th May 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:	3

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

General Data Protection Regulation

1. Purpose of the Report

1.1 The purpose of this report is to update the Police and Crime Commissioner on the preparations to implement the forthcoming Data Protection reform arising from the General Data Protection Regulation (GDPR) and the Data Protection Bill 2018, which incorporates Law Enforcement Processing and is awaiting Royal Assent.

2. Recommendations

2.1 The Strategic Resources and Performance Meeting is asked to note the contents of this paper

3. Reasons for Recommendations

3.1 To provide awareness of the current position of Nottinghamshire Police in terms of GDPR implementation.

4. Summary of Key Points

4.1 General Data Protection Regulations and Data Protection Bill 2018 (awaiting Royal Assent) comes into force on 25th May 2018

4.2 On a national level the National Police Chief's Council (NPCC) Lead for Information Management & Operational Requirements Co-ordination Committee (IMORCC), Commissioner Ian Dyson, continues to present reports to NPCC Chief's Council on the progress of the National Data Protection Reform Group. This group also provides updates to Force practitioners on the national group workstreams as below:

- **Data Protection by Design and National Systems** - to address standards for National Police Systems (including guidance for chief officers leading national projects) and Data Protection by Design. Working with the Police ICT Company and other relevant groups

- **Law Enforcement Database/GDPR transitions** – to understand the GDPR implications for this new national system working closely with Case Studies

representatives and colleagues from the Home Office and the Information Commissioner's Office (ICO).

- **Compliance Toolkit** – City Of London colleagues are continuing efforts to progress the procurement of a national compliance toolkit for use by all Forces.

- **Procurement and Data Processing Contracts** - this product will be circulated in the next update together with the products from part of the HR work assignment.

- **Emerging Issues -** negotiations are ongoing between NPCC, Home Office, ICO, Ministry of Justice, Criminal Prosecution Service and the Association of Police and Crime Commissioners regarding the disclosure of information to Victim Service Providers. A case study will be produced which reflects the outcome of these discussions at the earliest opportunity.

- **Update meetings -** of the National Data Reform programme took place at Ryton on 13th March 2018. A Regional Data Protection Reform seminar will take place at Derbyshire Constabulary on 3rd May 2018 where further updates from the national programme are expected**.**

4.3 On a local level Information Management Team staff have completed the self-assessment toolkit provided by the national team, created a terms of reference for a GDPR working group reporting to the Information Management Board, prepared a tactical communications plan and published the first comms message on the Force Intranet.

4.4 The local group has also reviewed the Force position in line with the ICO guidance, which highlights 12 steps organisations can take now to prepare for GDPR, the outcomes are as below:

- **Awareness** – to ensure all of the organisation's decision makers and key people are aware of the current changes in law – this is being addressed via the Communications Plan and GDPR Working Group

- **Information we hold** – to update the Information Asset Registers, review what data we hold, where it is stored, who has access to it, who it is shared with – this is beign addressed with a programme of visits to Information Asset Owners.

- **Information Charter (Privacy Notice)** – in line with the new code of practice released by the ICO . We need to review the current Information Charter and document what data is collected, who collects it, why, how will it be used and who we will share it with. All current notices currently displayed in all police facilities will need to be replaced, updated on the website and given orally over the phone or front counter where there is a need.

- **Rights of individuals** – The GDPR includes the following rights for individuals:
  - the right to be informed;
  - the right of access;
  - the right to rectification;
  - the right to erasure;
  - the right to restrict processing;

- the right to data portability;
- the right to object; and
- the right not to be subject to automated decision-making including profiling.

All Force records management processes relating to these rights will be reviewed and updated accordingly.

- **Subject Access** – The Information Management Team will be updating our procedures and planning how we will handle requests to take account of the new rules as below:
  - In most cases organisations will not be able to charge for complying with a request.
  - Organisations will have a calendar month to comply, rather than the current 40 days.
  - Organisations can refuse or charge for requests that are manifestly unfounded or excessive.
  - If organisations refuse a request, they must tell the individual why and that they have the right to complain to the supervisory authority (ICO) and to a judicial remedy. This must be done without undue delay and at the latest, within one month.

- The current Disclosure team is currently under review by the Business Improvement team, the main objectives of the review are as follows:
  - To determine the current processes with a view to improve the efficiency of these, where possible,
  - To determine the required FTE to ensure all Statutory Obligations and Service Level Agreements can be met.

- As our organisation handles a large number of access requests, we will also consider the logistical implications of having to deal with requests more quickly as part of this review.

- **Legal Basis for sharing** – Organisations will have to explain their lawful basis for processing personal data in their privacy notice and also when answering a subject access request. The lawful bases in the GDPR are broadly the same as the conditions for processing in the Data Protection Agreement. It should be possible to review the types of processing activities carried out and to identify the lawful basis for doing so. Organisations should document the lawful bases in order to help them comply with the GDPRs 'accountability' requirements – this requirement will be added to Information Asset registers

- **Consent** – As part of the Information Asset register refresh we will review how we seek, record and manage consent and whether the Force needs to make any changes. If individuals' consent is relied upon to process data, we will have to make sure that it meets the GDPR standard on being specific, granular, clear, prominent, opt-in, properly documented and easily withdrawn. If not, we will need to alter our consent mechanisms and seek fresh GDPR-compliant consent, or find an alternative to consent.

- **Children / Minor** – For the first time, the GDPR will bring in special protection for children's personal data. The GDPR sets the age when a child can give their own consent to this processing at 16 (although this may be lowered to a

minimum of 13 in the UK). If a child is younger then consent will be from a person holding 'parental responsibility'. There is need to ensure all systems have the capacity to verify the age of an individual and provide specific protection for children's personal data, - this requirement should also be identified on relevant Information Asset Registers.

- **Data Breaches** – The GDPR introduces a duty on all organisations to report certain types of data breach to the ICO, and in some cases, to individuals. Organisations only have to notify the ICO of a breach where it is likely to result in a risk to the rights and freedoms of individuals. If, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, organisations will also have to notify those concerned directly in most cases. Organisations should put procedures in place to effectively detect, report and investigate a personal data breach. They may wish to assess the types of personal data held and document where they would be required to notify the ICO or affected individuals if a breach occurred. Larger organisations will need to develop policies and procedures for managing data breaches. Failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself. To address this issue the Force Security Incident Reporting Policy, process and form have been updated and are available on the Intranet.

- **Data Protection by Design and Privacy Impact Assessments** – It has always been good practice to adopt a privacy by design approach and to carry out a Privacy Impact Assessment (PIA) as part of this. However, the GDPR makes privacy by design an express legal requirement, under the term 'data protection by design and by default'. It also makes PIAs – referred to as 'Data Protection Impact Assessments' or DPIAs – mandatory in certain circumstances. A DPIA is required in situations where data processing is likely to result in high risk to individuals, for example:
  - where a new technology is being deployed;
  - where a profiling operation is likely to significantly affect
  - individuals; or
  - where there is processing on a large scale of the special categories
  - of data

  To address this work will take place with the Business Change Team to start to assess the situations where it will be necessary to conduct a DPIA and identify:
  - Who will do it?
  - Who else needs to be involved?
  - Will the process be run centrally or locally?

- **Appointment of a Data Protection Officer** – The GDPR / new Data Protection Bill establishes new obligations for Chief Constables. One of which is the requirement to appoint a Data Protection Officer (DPO). The DPO must fulfil certain statutory responsibilities and be positioned at a suitable senior level within the organisation so as to operate independently, without influence, and report to the highest level of management.

  The role of the DPO has become increasingly important over recent years for information compliance and risk management, due to the substantial growth in

information held, system developments and multi-agency working, as referred to within the HMIC Report Building the Picture (pp 29-32), effective information management and compliance with data protection supports and improves operational efficiency and effectiveness.

Following a meeting with DCC Barber and Kevin Dennis it was agreed that the Force Information Management Lead will assume the statutory responsibility for Data Protection for both Nottinghamshire Police and Office of the Police & Crime Commissioner (OPCC).

- **International Data Transfers** – As part of the Information Asset Register refresh we will map out what we share outside of the UK and look at any data we are likely to share outside of the European Union (EU). The NPCC will be the lead for all forces where bulk data is shared with agencies such as Interpol. The Safe Harbour agreement will be abolished from May 2018 and the USA have agreed to sign up to the new Privacy Shield. There are thresholds to meet before considering sharing outside of the EU as below:

  - Article 45 - Adequacy - new list of countries that is "safe" to share with.
  - Article 46 – Safeguarding - USA and the Privacy Shield.
  - Article 49 – Exemptions - consent, contract, public interest, legal claim, vital interest and legitimate interest.
  - Extraterritorial – where business is conducted with overseas organisations, this now takes into account not only the country in which the data is being processed but the country in which the data subject resides. This also covers the storage of EU data in the cloud and ecommerce.

4 Financial Implications and Budget Provision

5.1 To monitor and review any financial implications for the shared Information Management Team roles including the new role of DPO in the delivery of and increased capacity required to provide professional knowledge and skills to review documentation and provide advice in ensuring that GDPR compliance is achieved by both Nottinghamshire Police and OPCC as each organisation is a separate legal entity.

5 Human Resources Implications

6.1 To monitor and review any resource implications for the shared Information Management Team roles including the new role of DPO in the delivery of and increased capacity required to provide professional knowledge and skills to review documentation and provide advice in ensuring that GDPR compliance is achieved by both Nottinghamshire Police and OPCC as each organisation is a separate legal entity.

6 Equality Implications

7.1 There are no equality implications arising from this report.

7 Risk Management

8.1 A GDPR risk, including the capacity issue, has been created and will be passed to DCC Barber for consideration in adding to the Strategic Risk Register.

8.2 Further risks identified through the Information Management and GDPR review process will be progressed through the Force and OPCC Corporate Risk Management processes.

8 Policy Implications and links to the Police and Crime Plan Priorities

9.1 Good Information Management will support the delivery of both the Chief Constable's and OPCC'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

9 Changes in Legislation or other Legal Considerations

10.1 The EU General Data Protection Regulation, including the UK Data Protection Bill 2018 becomes enforceable on 25th May 2018.

10 Details of outcome of consultation

11.1 No consultation has been required to complete this report.