Suffolk Police and Crime Commissioner

Making Suffolk a safer place to live, work, travel and invest

ORIGINATOR: CHIEF CONSTABLE	PAPER NO. AP14/41

SUBMITTED TO:	ACCOUNTABILITY AND PERFORMANCE PANEL – 18 JUNE 2014

SUBJECT:	COLLABORATION UPDATE – INFORMATION MANAGEMENT

SUMMARY:

1. Meetings of the Accountability and Performance Panel will receive update reports on the collaboration programme. It has been agreed that each report will focus on a particular department/ area of collaboration.

2. This report will focus on the collaboration within Information Management.

RECOMMENDATION:

1. The Accountability and Performance Panel is asked to note the content of this report.

1. KEY ISSUES FOR CONSIDERATION:

1.1. Meetings of the Accountability and Performance Panel will receive update reports on the collaboration programme. It has been agreed that each report will focus on a particular department/area of collaboration.

1.2. This report will focus on the collaboration within Information Management.

Background

1.3. In December 2013, former Deputy Chief Constable (Norfolk) and Assistant Chief Officer (Suffolk) commissioned the Strategic Change Department (SCD) to review current arrangements for information management across Norfolk and Suffolk Constabularies, with a view to collaboration.

1.4. A business case and structure for a new Joint Information Management Department (IMD) was submitted and approved by the Joint Chief Officer Team (JCOT) and PCCs in April 2013. The appointment of the Head of Information Management followed in September 2013 as part of change Tranche 8, to implement the collaborated department.

1.5. The following function areas that currently make up the IMD were phased across in Tranche 9 and report direct to the Head of Information Management with bases in Martlesham and Wymondham:-

1.5.1. Information Compliance Unit:

- Data Protection
- Freedom of Information (FOI) &
- Disclosure and Barring Service (DBS)

1.5.2. Information Security Unit

1.6. The Information Management collaboration also involved the movement of the PNC Bureau from Intelligence (Norfolk) to CJS during Tranche 9 and the changes remaining include:

1.6.1. Transfer of Crime Registry Unit to the Joint Performance and Analysis Department (JPAD), due to take place 2 June 2014, and

1.6.2. Finalisation of the structure of the Records Management Unit, within IMD which is currently planned in Tranche 10. In the interim, restricted duties officers presently working within the Norfolk Records Management Unit, transferred from Professional Standards to IMD 19 May 2014, to support the Joint Records Manager in the development of the Unit.

1.7. A series of meetings and projects are being progressed by the Units to harmonise the working practices to provide a single approach to Information Management across both forces.

1.8. The IMD Senior Management Team is in place. This is attached at Appendix A.

1.9. Force governance of information management has been revised and is delivered through the:

1.9.1. Joint Information Management Strategic Board, chaired on an alternating basis by the Deputy Chief Constables who also hold the role of Force Senior Information Risk Owner (SIRO), and

1.9.2. Joint Premises Security Working Group, chaired on an alternating basis by an Assistant Chief Constable of either force.

1.10. Work is underway to prepare for the planned audit of the Information Commissioner, in February 2015, with the intention of establishing the level of compliance across both forces and undertaking any necessary improvements. This will be a challenging piece of work and will span the Data Protection, Records Management and Information Security function areas.

1.11. At the April 2014 review, the Information Management collaboration savings were £112K. However this includes Crime Registry and PNC which do not form part of the collaborated IMD. There also remains the review of the Records Management Unit to incorporate within the IMD, which will involve the development of the Review Retention and Disposal of police information function to bring the forces to a level where they are compliant with the Management of Police Information (MoPI) Code of Practice and Guidance.

Information Compliance Unit

1.12. The Joint Force Information Compliance Manager was appointed 6 January 2014 and assisted in the development of the new structure incorporating the function areas that make up the Unit as outlined at 1.5.1.

1.13. Collective consultation took place on 23 April 2014 and no Data Protection and FOI staff were placed at risk.

1.14. The Disclosure and Barring staff were advised separately of the changes affecting their line management.

1.15. The new joint structure for Information Compliance went live on 5 May 2014. This is attached at Appendix B.

Data Protection/Freedom of Information

1.16. Work is underway to procure a joint case management system to provide a single method of delivery for both forces in response to individuals exercising their statutory rights of access to information under the Data Protection Act 1998 (DPA) and Freedom of Information Act (2000). An opportunity has since arisen for a 5 force procurement which is currently being considered. The case management system will provide additional efficiencies and improved management of information for both forces, enabling staff at either location to process requests on behalf of either force.

1.17. Since April 2014, data protection staff have been progressing a joint Annual Strategic Audit Plan 2014/15 which will see a single approach to data protection auditing and help monitor and improve the standard of data protection compliance in both forces.

1.18. The new structure aims to support the ongoing demand for Information Sharing to assist operational and investigative work and provide a central repository of signed information sharing agreements.

1.19. The new structure also aims to support information assets owners in delivering compliance and management of their information.

1.20. A series of meetings and workshops are now taking place with staff to harmonise working practices, policies and procedures.

1.21. Both functions currently respond effectively to requests for information which is demonstrated by high performance figures.

Disclosure and Barring (Including Common Law Police Disclosures)

1.22. Both teams are externally funded by the Disclosure and Barring Service. Work is underway to harmonise working practices and decision making authority levels.

1.23. Both forces are demonstrating excelling performance and hitting all nationally set service level achievement targets.

1.24. Further work is required to harmonise the common law police disclosures (force funded) line management reporting lines.

Information Security Unit

1.25. The Joint Force Information Security Manager was appointed 3 March 2014, who will be supported by an Information Security Advisor (recruitment is in progress) to complete the Information Security Unit establishment.

1.26. Work is underway to address the Cabinet Office Security Policy Framework (SPF) and Information Standards, which all UK forces are mandated to follow. The SPF is aligned with Her Majesty's Government (HMG) ISO 27001 (International Information Security Standard) and used to set the minimum security baseline and Information Assurance Maturity Model (IAMM) to inform an organisation whether security culture and practice are embedded within business processes.

1.27. Further work is underway to progress the required annual returns to the National Police Information Risk Management Team (Home Office), known as a Protective Security and Risk Management Overview. The returns cover a number of specific areas including, details of the organisational security, delivery partners and third party suppliers, HMG Mandatory Requirements, Community Security Policy and Code of Connection which stipulate the minimum security requirements in order to be connected to the Criminal Justice Extranet (CJX). Completion and submission of the annual Home Office return is due at the end of May 2014. Subject to satisfactory independent technical testing this is currently on schedule for delivery.

1.28. Information security within Norfolk and Suffolk Constabularies has been developed with different interpretations, cultures and attitudes.

1.29. A number of joint Information Security policies/procedures were issued late 2012 early 2013. These are now under review to ensure they reflect the organisational changes that have taken place since then. Where possible, the policies and processes are developed as joint although there are some difficulties where this involves existing contracts or either force has deeply embedded processes to address the same business area. These are referenced within documentation and will form part of the longer term collaborative approach.

1.30. Information Security related business processes are also being reviewed to ensure that they meet recognised industry best practice, regulatory and legislative requirements.

1.31. Internal Information Security audit is limited and work is underway to rectify the requirement for an independent information security audit to be conducted.

1.32. The new Government Security Classification Policy (GSCP) is due to be adopted by police forces in October 2014. There is a Home Office project team assisting on this and will involve training requirements across the Constabularies. The Home Office and police service also recognise that risks exist around the handling and sharing of data within current sensitive systems. These issues are yet to be resolved and futther guidance is awaited.

1.33. Police services have begun the transition from the current Criminal Justice Extranet (CJX) (equivalent to GSX) to the new Public Services Network (PSN). There is significant work required by ICT in order to meet the PSN Code of Connection which is overseen by Cabinet Office. Cabinet Office is currently operating a zero tolerance approach which means that controls within the Code of Connection must be met. Information Security has close and regular contact with the Home Office Public Services Network in Policing project team as well as the National Accreditors for police systems. The transition to PSN must be completed by October 2015 which given scale of work is a very tight deadline.

Records Management Unit

1.34. The Joint Force Records Manager was agreed in post on 10 February 2014.

1.35. Work is underway to improve the effective management of force records to aid operational efficiency and meet legal and statutory obligations around information management. The extent of the work will include the harmonisation of the force Review, Retention and Disposal (RRD) procedures in respect of personal information covered by the Data Protection Act 1998. (DPA)

1.36. The primary purpose of RRD is to protect the public and help manage the risk posed by known offenders and other potentially dangerous people. To that end, the Constabularies have a responsibility to regularly review the nominal records and apply the principles of the Management of Police Information (MoPI) Code of Practice and Guidance in order to assess risk and prioritise high risk offenders. This includes electronic and paper records relating to offenders, suspects, victims and witnesses that are held in both structured and un-structured data sources.

1.37. Early work is underway, assisted by Strategic Change to explore the benefits and costs of an automated solution to help administer the high volume RRD process.

1.38. Further work is imminent to improve the corporate tracking of police records and review the volume of files in off-site archive.

Current Performance Issues

1.39. There is a backlog of work in information security associated with external audit requirements and the annual information security returns to the National Police Information Risk Management Team (Home Office). The Information Security Manager is addressing this.

1.40. There is further work to undertake to fully implement the Management of Police Information (MoPI) Code of Practice and Guidance in both forces. HMIC have commenced a MoPI inspection of forces, although there are no dates as to when Norfolk and Suffolk may come under scrutiny.

1.41. In regards the above two points this appears to be a similar position for other forces across the country.

1.42. With the exception of the case management system (see 1.43 below), there are currently no significant performance issues associated with data protection, freedom

of information and disclosure and barring. The growing disclosure demand is under constant review.

Issues as a result of collaboration

1.43. Source Systems/Case Management System - The effectiveness of the IMD is dependent on the integration of and access to source systems across both forces which is compatible with a joint case management system. Once this has been achieved, staff will benefit from full interoperability and be able to process cases at either location on behalf of either force.

1.44. Windows XP - Suffolk Data Protection and Freedom of Information staff currently operate on a Windows XP platform as the case management system in use is incompatible with the Windows 7. ICT are developing an interim solution until the replacement of the case management system. With the exception of minor functionality issues and some failure of service, this is manageable at present.

1.45. Staff Abstraction - The development of any information system requires expert advice from information management specialists. With limited expertise available within the IMD, any abstraction of skilled staff has a large impact on their capacity to deliver business as usual. This is particularly problematic for the Information Security Unit which comprises of 2 FTE.

1.46. Mail/Web Marshall - The variation of rules on the Electronic Mail and Web Marshall system have proved challenging and currently absorb a considerable amount of the Information Security Manager's time in the release of the information for business and operational purposes. Work is in progress to reduce the time spent through a technical re-configuration of the rules.

Current risks and actions undertaken to mitigate them

1.47. Specialist staff (Resilience) - Workload associated with the change programme and development of new systems has an impact on specialist staff within the IMD which carries a risk that demand may outstrip resources. At present, there are limited numbers of specialist staff and within budgetary constraints, ongoing staff development is undertaken to improve expertise and resilience. Resources are kept under constant review and any shortfalls which are impossible to meet in-house are raised with Chief Officers for consideration of additional temporary resources.

1.48. Records Management – The lack of a joint approach in Records Management currently creates inefficiencies and inconsistencies in the MoPI RRD process which limits the availability of full information for operational policing. This also heightens the challenge of non-compliance with the Data Protection Act 1998. The Records Manager is developing a strategy to improve this position for both forces. Further work is being explored to identify benefits and costs of an automated solution.

2. FINANCIAL IMPLICATIONS:

2.1 Non - compliance with the Data Protection Act 1998 can result in a maximum monetary penalty of £500,000.

3. OTHER IMPLICATIONS AND RISKS:

3.1 No changes are needed to the PCC risk register.

ORIGINATOR CHECKLIST (MUST BE COMPLETED)	PLEASE STATE 'YES' OR 'NO'
Has legal advice been sought on this submission?	No
Has the PCC's Chief Finance Officer been consulted?	No
Have equality, diversity and human rights implications been considered including equality analysis, as appropriate?	Yes
Have human resource implications been considered?	Yes
Is the recommendation consistent with the objectives in the Police and Crime Plan?	Yes
Has consultation been undertaken with people or agencies likely to be affected by the recommendation?	N/A
Has communications advice been sought on areas of likely media interest and how they might be managed?	No
Have all relevant ethical factors been taken into consideration in developing this submission?	Yes