Joint

Information Management

Strategy (IMS)

TABLE OF CONTENTS

1.   INTRODUCTION

1.1   Bedfordshire Police, Cambridgeshire Constabulary and Hertfordshire Constabulary (BCH) have a duty to obtain and use a wide variety of information in order to discharge their duties effectively and keep people safe.

1.2   Information management describes the means by which these Forces efficiently plans, collects, organises, uses, controls, disseminates, retains and disposes of information, and through which it ensures that the value of that information is identified and exploited to the fullest extent.

1.3   It is intended that the Information Management Strategy (IMS) will be dynamic: IMS related projects and work streams will change over time to meet the needs of the Force and national developments in policing.

1.4   The IMS should be seen in the context of national developments across the police service and in particular: the prevailing imperatives to create and maintain national police databases.

1.5   Although the IMS covers all information held by the three Police Forces, it is primarily concerned with police information. Police information is information required for a policing purpose, which is defined by, as necessary for:

- Protecting life and property
- Preserving order
- Preventing the commission of offences
- Bringing offenders to justice
- Any duty or responsibility arising from common law or statute law

1.6   These five policing purposes provide the legal basis for the collecting, recording, evaluating, sharing and retaining of police information.

1.7   The IMS is not a stand-alone strategy. It is intrinsic to how the Force manages all of its police information within the policing context and as such informs, and is informed by, all other Force policies. The Forces have an Information Management Policy, to which all record management procedures will be linked.

1.8   Safeguards to the information held by the Force will be provided through the BCH Information Security Policy and through compliance with other national and local policy and standards.

1.9   The IMS has been drawn up within the context of: Authorised Professional Practice (APP) for Information Management, the Data Protection Act 1998, the Freedom of Information Act 2000, and takes into consideration the information management principles as defined by the International Standard Organisation (ISO) 15489.

1.10   The Force will work within a regulatory environment complying with relevant and related legislation, statutory instruments, Common Law and Codes of Practice.

2.   SCOPE

2.1   The IMS relates to all police information (including digital images) held by the Force in whatever format. This includes information which supports the Force in achieving its statutory policing functions as well as the administrative functions of HR, finance, fleet etc.

2.2   The priority of the IMS is police information held in six business areas identified in the APP for Information Management namely: Crime; Intelligence; Domestic Violence; Child Protection; Custody and Firearms. These areas prioritise the higher risk offenders and represent the most significant risk in relation to children and vulnerable adults.

2.3   The foregoing are national priorities across the police service, which will help the service prepare for the sharing of police information.

2.4   Data quality is fundamental to successful information management. It is essential that information is recorded properly at the outset. All police information must conform to the following data quality principles: accurate, adequate, relevant, and timely.

3.   STRATEGIC AIMS and OBJECTIVES

3.1   Our strategy is to provide clear direction, support and commitment to the discipline of Information Management across the three Forces.

3.2   Aim:
- To meet the required standards to comply with relevant legislation, Force and national policies, including Code, Guidance and Standards.
- To meet national policing requirements in order to support information sharing including through national police databases.
- To develop effective records management.
- To improve police performance by ensuring information is reliable, accessible and available at the point of need.

3.3   Objectives:
- To create and maintain relevant Force polices and procedural guidance.
- To develop the necessary IT infrastructure to support local and national developments including mobile data.
- To adopt and develop systems to support the concept of the 'Prime Record' and the basis for records management.
- To implement and develop a process for review of records.
- To reduce the number of information silos, by ensuring records are linked and in a format which is searchable.
- To create and store more records electronically.

- To reduce the number of paper records held by the Force and to develop appropriate storage systems.
- To apply the Force Information Management Principles (section 4).

4.   INFORMATION MANAGEMENT PRINCIPLES

4.1   The Forces will meet their responsibilities by managing information consistent with legal and ethical obligations, and according to its value.

4.2   Information will be obtained and managed effectively for a policing purpose complying with the principles of the Authorised Professional Practice (APP) for Intelligence Management and National Intelligence Model (NIM).

4.3   Information will be accurate and up to date and of appropriate quality to support operations and the decision-making process. Where possible duplication will be avoided.

4.4   Information must be readily accessible and understandable to those who need it for operational or business reasons, to enable staff to carry out their duties.

4.5   Information will be managed securely, ensuring the continuity of operations and minimising the possibility of damage to service provision by limiting the impact of security threats or incidents, whether internal, external, deliberate or accidental.

4.6   Information shared with partner agencies will be carried out in accordance with the relevant legislation and guidance and recorded in accordance with Force procedures. Where information is to be shared on an on-going basis an Information Sharing Agreement (ISA) should be signed by the parties. Information Sharing Agreements will be stored in an accessible and searchable format on each individual Force Intranet Sites.

4.7   Information which is disclosed on a case by case basis will be disclosed in accordance with relevant legislation, and recorded as per Force procedures.

4.8   Information will form part of usual operational business, be integrated and consistent across all business areas within the Forces.

4.9   Information will be reviewed in an informed and well-governed process, which takes account of current legislation and national guidance. The individual Force review, retention and disposal procedure will document this process.

4.10   Information will be retained in an accessible format which will should be easily retrieved and made available to all officers and staff employed by the Force. Information that has reached its lifecycle end will be disposed of in a secure manner and in accordance with Force policy and procedures.

5. THE ROLE OF THE INFORMATION MANAGEMENT STRATEGY GROUP (IMSG)

5.1   The IMSG, chaired by the Deputy Chief Constables (DCC), has an overarching role in providing the strategic drive, direction, coordination, control and approval necessary to achieve the strategic aims and objectives of the IMS (see Appendix a – Terms of Reference for Information Management Strategy Group (IMSG)).

5.2   The IMSG will monitor and direct work streams applying the IMS to key operational business areas thereby ensuring delivery of the Strategy.

5.3   The IMSG will liaise with other strategic groups in the Forces through the attendance of appropriate IMSG members at those groups to ensure a corporate strategy for information management.

5.4   The IMSG will approve the Force Risk Assessed Audit Plan, which will measure compliance with the Data Protection Act and the APP for Information Management with particular attention to data quality and actions identified by the project groups to improve the availability of relevant information and reduce risk.

5.5   The IMSG will ensure that the Force Training Strategy is aimed at the training of police officers and police staff in the guidance on the Management of Police Information (APP for Information Management) and data integrity.

5.6   The IMSG will ensure that the IMS is available for all staff, partners and the public to view. It will give guidance for good information practice and will promote compliance with this strategy so that police information will be accessed easily, appropriately and in a timely manner.

6. RESPONSIBILITIES

6.1   The Chief Constables of Bedfordshire Police, Cambridgeshire Constabulary and Hertfordshire Constabulary are the data controllers for their respective Forces. This role is defined in the notification which the Forces have made as required by the Data Protection Act 1998 and is the individual within the organisation who determines the purpose and manner in which personal data is processed.

6.2   The DCC has been delegated the responsibility for central oversight of all information held by the Force. This role is accountable to the Chief Officer for the everyday management of police information within the Force.

6.3   Each individual Head of Information Management will oversee the implementation and compliance of the Force Information Management Strategy. This includes the co-ordination of any strategic work strands specialist advice and support to the organisation whilst leading on and recognising areas of improvement and compliance relating to Information Management.

6.4   The Head of Training is responsible for the implementation of the Force Management of Police Information Training Strategy. The Head of Information Management and The Head of Training will liaise and identify additional training needs relating to the IMS and APP for Information Management

6.5   Business owners are responsible for all aspects of information management within their business area, this includes ensuring that information management policies, processes and procedures are followed, data quality

standards met, review, retention and disposal procedures are followed, appropriate security applied and benefits realised.

6.6   All staff within each Force will ensure that all information created, reviewed and held for which they are responsible is accurate, relevant and kept up to date. All staff will:

- apply the basic principles of effective information management as contained in Authorised Professional Practice

- apply the data quality principles to all police information

- apply the operating rules relevant to the business areas to which they have access

- apply the rules relating to information security

- ensure compliance with all relevant legislation, including the Human Rights Act 1998, Data Protection Act 1998 and Freedom of Information Act 2000.

7.   WHO TO CONTACT ABOUT THIS STRATEGY

7.1   Questions regarding this Strategy and its operation should initially be referred to your Force Information Management team:

- BCH Information Rights, Bedfordshire Police Headquarters, Kempston. MK43 9AX.
  Tel 01234 842547

Appendix a – Terms of Reference for Information Management Strategy Group (IMSG)

Remit of the IMSG

- To ensure that information held for a policing purpose is accurate, adequate, relevant, timely and not excessive
- To ensure that information owned by *Bedfordshire Police / Cambridgeshire Constabulary / Hertfordshire Constabulary* (delete as applicable) or 'the Force' is held legally, securely, ethically and can be appropriately shared
- To produce and manage Information Management Systems
- Set and review strategic audit plans

Relationship to other groups

The IMSG acts as a strategy group (Gold) to set direction for the operationally focussed activities of the CMS User Group (CUG).

Responsibilities

The IMSG has strategic responsibility for the:

- Information Management Strategy and Information Management Policy
- Decisions on the purchase of information systems in the Force to ensure that the number of information silos are reduced and that operational information (whenever possible) can be linked
- Data Sharing (via the Information Management Policy)
- National Crime Recording Standards (NCRS) and Crime Data Integrity
- Issues arising at the CUG that need to be referred for resolution
- Audit and compliance plans and direction
- Information items arising from the Force strategic Risk Register

Membership

- Force Senior Information Risk Owner (SIRO) - DCC
- Force Chief Information Officer
- Head of ICT (or nominee) as required
- Crime & Incident Registrar (Cambridgeshire) or Deputy Crime Registrar (Bedfordshire) or an appropriate representative from their team
- Public Protection Unit (PPU) SPoC
- Crime SPoC
- Intelligence SPoC
- Criminal Justice SPoC

- Special Branch SPoC (Not in Cambridgeshire)
- Project Management representative when required
- Other Business Area representatives when required

Note: Additional attendees may be invited when particular issues are under consideration or they are needed to report on progress or answer questions.

Frequency of Meetings

Bi-monthly or as dictated by need.

Standing agenda items

1. Information Management related projects
2. Issues from CUG (not applicable for Cambridgeshire)
3. NCRS and Crime Data Integrity
4. Audit reports
5. Information strategy and related policies including Data Quality
6. National information-related publications for attention / action in force to determine ownership

Appendix A

DRAFT - BCH Information Management Board (IMB) Terms of Reference (ToR)

Title	BCH IMB ToR
Author	Head of IMD – Andy Gilks
Owner	Director of Information - Ian Bell
Version No	V 0.1
Classification:	Official
Date	07/02/2017

Purpose

- To ensure that information held for a policing purpose is accurate, adequate, relevant, timely and not excessive
- To ensure that information owned by the three forces Bedfordshire, Cambridgeshire and Hertfordshire (BCH) is held legally, securely, ethically and can be appropriately shared
- To produce and manage Information Management Systems (IMS)

Responsibilities

- Information Management Strategy, the Data Quality Strategy and Information Management Policy
- Decisions on the purchase of information systems in the force to ensure that the number of information silos are reduced and that operational information (whenever possible) can be linked
- Data Sharing (via the Information Management Policy)
- Information items arising from the BCH Strategic Risk Register
- Ensure best practice is followed from the Information Commissioners Office (ICO) and the APP on Information Management
- Ensure compliance with the standards on disclosure from the Disclosure & Barring Service (DBS)

Attendees

BCH SIRO	Head of IMD
Head of MOPI	Head of Information rights & Assurance
Head of DBS	Head of Professional Standards or nominee
Head of ICT or nominee	Strategic lead for Athena or nominee
A named representative from Beds, Cambs & Herts	A named representative from CT and ERSOU
Head of Learning & Development	Project Management representative when required

Other Business Area representatives when required	Additional attendees may be invited when a particular issue is under consideration

BCH IMB Standing Agenda

1. IMD update

   - MOPI/Records Management
   - Information Rights
   - DBS
   - Athena

2. Information Management Strategy and related policies

3. Data Quality

4. National information-related publications for attention / action in force to determine ownership

Terms of Reference will be reviewed after 6 months of operation