Information management index

Contents

Management of police information

Collection and recording

1 Collection

1.1 Means of information collection

1.1.1 Routine collection

1.1.2 Volunteered information

1.2 Key roles in collection

2 Recording

2.1 Crime recording

2.1.1 National crime recording standard

3 Incident record

3.1 Case and custody

3.2 National firearms licence management system

3.3 Considerations

3.3.1 Principles

3.3.1.1 Government protective marking scheme

3.3.1.2 Data quality principles

3.3.2 Categorising police information

3.3.2.1 Person records

3.3.3 Establishing a person’s identity

3.4 Key roles in recording

Evaluation

1 Principles

2 Evaluating records

3 Action management

4 Key roles for the evaluation of information

Common process for managing police information

1 Common process at force level

2 Management of police records

3 Critical information areas

3.1 Public protection

4 Certain public protection matters

5 Information management strategy

6 Responsibilities for managing police information

Sharing police information

1 Information sharing

2 Statutory obligation to share information

3 Statutory power

4 Common law

4.1 Dissemination

4.2 Common law duty for confidentiality

4.2.1 Personal or sensitive information

5 How the police share information

6 Proportionality when sharing personal information

7 Information sharing agreement

7.1 ISA process chart

7.1.1 Has a legal duty or power been identified?

7.1.2 Identify the partners with whom the information will be shared

7.2 Setting out the process for sharing information

7.2.1 Who will approve and authorise the ISA?

7.2.2 Where will the ISA be held?

7.3 ISA review process

7.3.1 Stage 1 – does the agreement have the right contact list?

7.3.2 Stage 2 – is the agreement still useful and fit for purpose?

7.3.3 Stage 3 – has the review identified any emerging issues?

7.3.4 Stage 4 – extending/terminating the agreement

8 Sharing outside an ISA

9 Key roles in the sharing of information

Retention, review and disposal

1 Retention

1.1 Deciding to retain

1.2 Which records should not necessarily be retained

1.2.1 Retaining intelligence products

1.3 National retention assessment criteria

1.3.1 NRAC questions

2 Review

2.1 Initial review and evaluation

2.2 Triggered reviews

2.2.1 When should a triggered review take place?

2.3 Scheduled reviews

2.3.1 Group 1 – certain public protection matters

2.3.2 Group 2 – other sexual, violent or serious offences

2.3.2.1 Sexual offences

2.3.2.2 Violent offences

2.3.2.3 Serious offences

2.3.3 Group 3 – all other offences

2.3.4 Group 4 – miscellaneous

2.3.5 Review schedule

2.4 Exception reviews

2.5 Clear periods

2.6 Audit and supervision of the review process

2.6.1 Annual inspections and monthly audits

2.6.2 Documenting the review process

2.6.3 Authorising the review process

2.7 Key roles in the review of information

3 Disposal

3.1 Audit

Freedom of information

1 Obligations and responsibilities

1.1 Public authorities

1.2 NPCC national policing freedom of information and data protection central referral unit

1.3 Information Commissioners Office

1.4 Forces

1.5 Freedom of information officer

2 Freedom of information request process

2.1 Information liable for disclosure

2.2 Information not liable for disclosure

2.3 Requests

2.4 Dealing with a request

2.5 Fees and charges

2.6 Timescales

2.7 Responding to the applicant

2.7.1 Internal review and appeals

2.8 Vexatious and repeated requests

2.9 Transferring the request

2.9.1 Consultation with third parties

2.10 Decision making process

2.10.1 Stage 1 – information gathering

2.10.2 Stage 2 – neither confirm nor deny

2.10.3 Stage 3 – harm

2.10.4 Stage 4 – exemptions

2.10.5 Stage 5 – public interest test

3 Freedom of information exemptions

3.1 FOIA section 21 – information reasonably accessible by other means

3.2 FOIA section 22 – information intended for future publication

3.3 FOIA section 23 – information supplied by, or relating to, bodies dealing with security matters

3.3.1 Relationship between section 23 and section 24

3.4 FOIA section 24 – national security

3.4.1 Ministerial certificates

3.5 FOIA section 27 – international relations

3.6 FOIA section 28 – relations within the UK

3.7 FOIA section 29 – the economy

3.8 FOIA section 30 – investigations and proceedings conducted by the public authority

3.8.1 Historical investigation records

3.8.2 Relationship between FOIA section 30 and 31

3.9 FOIA section 31 – law enforcement

3.10 FOIA section 32 – court records

3.11 FOIA section 36 – prejudicing the effective conduct of public affairs

3.12 FOIA section 37 – communication with the royal family and honours

3.13 FOIA section 38 – health and safety

3.14 FOIA section 39 – environmental information

3.15 FOIA section 40 – personal information

3.16 FOIA section 41 – information provided in confidence

3.17 FOIA section 42 – legal professional privilege

3.18 FOIA section 43 – commercial interests

3.18.1 Contracts/confidentiality clauses

3.19 FOIA section 44 – prohibitions on disclosure

4 Force publication scheme

4.1 Guide to published information

4.2 Monitoring and reviewing the force publishing scheme

4.3 Complaints procedure

5 Environmental information regulations

Data protection

1 Data protection introduction

1.1 Legal definitions

1.2 Personal data in a policing environment

1.2.1 Anonymised data

1.3 Processing in a police environment

2 Governance

Data protection principles

1 Principle 1 – fair and lawful processing

6.6.4 Updating force records from subject access requests

6.6.5 Multiple/duplicate previous subject access request

6.6.6 Subject access requests from members of staff

6.6.7 Requests for additional information

6.6.8 Failed job applicants

6.6.9 Joint applications

6.6.10 Non-specific applications

6.6.11 ANPR

6.6.12 Fee waiving

6.6.13 CCTV

6.6.14 Undetected crime reports

6.7 Right to prevent processing likely to cause damage or distress

6.8 Preventing direct marketing

6.9 Automated decision taking

6.10 Compensation

6.11 Correcting inaccurate personal data

6.12 Requesting an assessment from the Information Commissioner

6.13 Complaints and resolutions

7 Principle 7 – security and protective measures

7.1 Data processing contract

7.2 Data protection/information system operating rules

7.3 Security of personal data in decommissioned police premises

8 Principle 8 – transfer outside the European Economic Area

Audit

1 Roles and responsibilities

1.1 Data controller

1.2 Senior information risk officer

1.3 Information asset owner/senior system owner

1.4 System administrator

1.5 Compliance auditors

1.6 Regional and national audit groups

2 Data quality

2.1 High quality and known quality

3 Compliance audit

4 Monitoring

4.1 Monitoring of record update/creation

4.2 Recording of monitoring

5 Transaction validation

5.1 Method

5.2 Sample size – access to data/transaction checks

6 Self-inspection

6.1 Self-inspection package

7 Risk assessment

7.1 Risk assessment process

7.1.1 Completion of the risk assessment

7.1.2 Risk assessment outcome

8 Audit programme (plan)

8.1 Practical audit phase

8.1.1 Planning the audit

8.1.2 Communication with the business owner

8.1.3 Terms of reference

8.1.4 Process maps

8.1.5 Testing phase

8.1.5.1 Supporting/substantiating force records

8.1.6 Reporting the audit findings

8.1.7 Post-audit review

8.2 Retention of audit documentation

Information assurance

1 Introduction

2 Governance

2.1 Information risk management structure

2.2 Functions and responsibilities

2.2.1 National senior information risk owner

2.2.2 Senior information risk owner

2.2.3 National police information risk management team

2.2.4 Police information assurance board

2.2.5 Information asset owner

2.2.6 Information security officer

2.2.7 Accreditor

3 National policing community security policy

3.1 Aims of the community security policy

3.2 Community security policy compliance

4 Protective security risk management overview

5 The community code of connection

6 Accreditation

7 Management of information risk

7.1 Risk appetite

7.2 Residual risk

8 Risk escalation case

9 Information security incidents – reporting and monitoring

10 Police warning, advice and reporting point

Linked reference material

First published: 12 December 2013 **Last modified:** 14 January 2016