POLICY

Information Management

Policy Owners	Head of Information Management
Policy Holder	Head of Information Management
Author	Head of Information Management

Policy No.	116

Approved by

Legal Services	✓ 20.01.16.
Policy Owner	✓ 29.01.16.
JJNCC	✓ 15.09.15.

Note: *By signing the above you are authorising the policy for publication and are accepting responsibility for the policy on behalf of the Chief Constables.*

Publication date	02.02.16.
Review date	02.02.18.
APP Checked	✓ 19.01.16.

Note: *Please send the original Policy with both signatures on it to the Norfolk CPU for the audit trail.*

Index

Legal Basis

(Please list below the relevant legislation which is the legal basis for this policy). You must update this list with changes in legislation that are relevant to this policy and hyperlink directly to the legislation.

Legislation/Law specific to the subject of this policy document

Section	***Act (title and year)***
	Common law duty of confidentiality

Other legislation/law which you must check this document against (required by law)

Act (title and year)
Human Rights Act 1998 (in particular A.14 – Prohibition of discrimination)
Equality Act 2010
Crime and Disorder Act 1998
H&S legislation
Data Protection Act 1998
Freedom Of Information Act 2000
Bribery Act 2014
Common law duty of confidentiality
Computer Misuse Act 1990
Copyright, Designs and Patents Act 1988
Criminal Procedure and Investigations Act 1996 (CPIA)
Obscene Publications Act 1959

Official Secrets Act 1911 – 1989
Protection of Freedoms Act 2012
Regulation of Investigatory Powers Act 2000 (RIPA)

Other Related Documents

- Information Security Policy
- Records Management Policy
- Data Protection Policy
- Freedom of Information Policy
- Information Sharing Policy
- Information Risk Management Policy
- Information Asset Owners Policy
- Force Risk Appetite Statement
- Data Quality Policy
- DBS & CLPD Policy
- Requests for removal of DNA, Fingerprints and PNC records (Exceptional Case) Procedure
- Information Audit and Monitoring Procedure
- Information Management Training Procedure
- College of Policing Code of Ethics
- Norfolk and Suffolk Constabularies' Standards of Professional Behaviour
- Information Commissioner's Office (Guidance)
- College of Policing Authorised Professional Practice
- ACPO Manual of Freedom of Information 2000
- ACPO/ACPO Information Systems Community Security Policy (CSP)
- ACPO/ACPOS Accreditation Policy for National Police Systems
- Statutory Code of Practice on the Management of Police Information (MoPI).
- HMG Security Policy Framework and Communications Electronic Security Group (CESG) information Standards and notices.

1. Policy Aim

1.1 This policy aims to support Norfolk and Suffolk Constabularies to provide the right information at the right time for the right reasons to the right people, through the effective management of its information.

1.2 This policy aims to provide clear direction, support and commitment to the discipline of Information Management for Norfolk and Suffolk Constabularies by detailing how information gathered for policing will be collected, recorded, evaluated/actioned, shared, reviewed, retained and disposed of.

1.3 This policy is supported by a series of interrelated policies and procedures that further detail how other matters connected with the management of information takes place, such as; security accreditation, legal procedures for data handling; standards of control and accountability, provision of access to information, safe disposal, standards of compliance.

2. Applicability

2.1 This policy applies to all information held and used by Norfolk and Suffolk Constabularies including that used for policing duties and for administrative purposes such as HR, Finance, fleet, etc.

2.2 This policy applies to Norfolk and Suffolk personnel including police officers, police staff, special constables, volunteers that use the constabularies' information as necessary to carry out their *policing duties* and to contractors, partner agencies and other individuals who may have access to either constabulary's information for the purpose of carrying out their *policing duties*.

2.3 For the purpose of this policy, ***'policing duties'*** will assume the same definition as the Code of Practice for the Management of Police Information gives for it:

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

3. The Policy

3.1 Norfolk and Suffolk Constabularies recognise that the collection of appropriate information with a high standard of data quality, its accurate assessment and timely exploitation are core to efficient policing.

3.2 The Constabularies are committed to implementing legislation and guidance with particular emphasis on maximising the benefits effective information management brings to operational policing.

4. Information Management Governance

4.1 The Chief Constables of Norfolk and Suffolk Constabularies are the **Data Controllers** and ultimately accountable for their respective information.

4.2 The **Senior Information Risk Owners (SIRO)** are the Deputy Chief Constables of Norfolk and Suffolk Constabularies who hold the delegated responsibility for:

- Chairing the Joint Information Management Strategic Board (JIMSB),
- Oversight of this Policy through the JIMSB,
- Setting the Constabularies' (Local) Risk Appetite Statement,
- Leading the management of information risks for policing within their constabulary,
- Leading and fostering a culture that values, protects and uses information for the public good,
- Owning the information risk policy and risk assessment process,
- Advising the Chief Constable on information risks and taking and/or accepting risk based decisions in respect of the manner in which information is to be managed within their constabulary.

4.3 The **Joint Information Management Strategic Board (JIMSB)** will meet approximately every 6 weeks for which a terms of reference will exist.

4.4 An **Information Management Department** lead by the Head of Information Management will provide information management support and advice in the following areas: Data Protection, Freedom of information, Records Management, Information Security, Information Sharing, Information Compliance, Disclosure and Barring (including common law police disclosures).

4.5 **Information Asset Owners** will be appointed and are responsible for the effective management of information assets falling within their responsibility. Information Assets Owners will be supported by an appropriate policy, guidance and training.

5. Information Management Strategy (IMS)

5.1 A joint Force Information Management Strategy will be produced and maintained under the direction of the Deputy Chief Constables. W:\Collaboration\InformationManagement\InfoMgmtCommand\Org\Governance\Information Management Strategy 2014-2017

5.2 The Information Management Strategy (IMS) will set out:

- Who is responsible for the Information held by the constabularies.
- The purpose for collecting and holding information.
- Which business areas hold information within the constabularies and the standards that will apply (Information Asset Register).
- The safeguards applied to police information (Information Asset Register).
- The relationship between police information held within different business areas (Information Asset Register).
- Which processes ensure that police information is audited for accuracy and relevance to the policing purposes (Notification requirements).
- The controls that are applied to ensure the integrity and security of police information held by the constabularies (Notification requirements and RMADS etc).
- The training required to support the management of police information.
- The dedicated resources which support the delivery of the IMS and their relationship to other business areas.
- Arrangements for receiving records and monitoring record keeping, and
- How the constabularies comply with national and local security policy and standards.

6. Use of Information

6.1 All Information held by Norfolk and Suffolk Constabularies is for the purpose of policing within both Counties and the wider police community. The information is for use by all individuals mentioned above for the purpose of their official policing duties. Individuals are not permitted to use the information:

- For their own personal gain,
- Out of casual curiosity,
- For another person's curiosity, and
- For any reason other than as permitted to perform their current duties.

6.2 There is an expectation of trust on individuals to handle Norfolk and Suffolk Constabulary information appropriately and with due care and diligence.

6.3 Individuals will be called upon to justify their actions, if deemed necessary. This can occur through means such as routine auditing/monitoring or

following a compliant/misconduct/discipline enquiry or through the progression of an investigation.

6.4 Feedback will be provided to staff who do not handle information in accordance with this policy and where necessary, ***appropriate disciplinary action and/or criminal investigation will take place. A referral to the Information Commissioner may also take place.***

Personal use of email and Internet

6.5 The Constabularies internet and email is intended for Constabulary use only; personal use of the internet is not permitted and should only be used by authorised individuals with a policing purpose. (See Email, Internet and Intranet Use Policy).

Information Charter

6.6 An Information Charter will be produced and published on each Constabulary website.

7. Information Management Areas of Business

7.1 Information Management covers a number of discrete but interrelated areas of business and the following sections offer a brief policy statement for each of these areas:

- Management of Police Information (MoPI)
- Data Protection
- Data Quality
- Audit and Monitoring
- Information Security
- Records Management
- Freedom of Information
- Information Sharing
- Disclosure of Information
- Information Compliance and Handling Information Disputes
- Information Management Training

8. Management of Police Information (MoPI)

8.1 Norfolk and Suffolk Constabularies are committed to complying with the Code of Practice for the Management of Police Information[1] and it's supporting Guidance.

[1] http://library.college.police.uk/docs/homeoffice/codeofpracticefinal12073.pdf

8.2 Authorised Professional Practice (APP) for Information Management[2] is used as general guidance to support the Constabularies application of the MoPI principles.

9. Data Protection Act 1998

9.1 Norfolk and Suffolk Constabularies remain separate Data Controllers and are committed to ensuring that Officers, Staff, Specials and Volunteers undertake their legitimate duties in a manner that is compatible with the Data Protection Act 1998 and will endeavour to ensure that the data protection principles are applied to all personal information held and used by both the constabularies. However, in the event of jointly collaborated functions they may indeed become joint Data Controllers. This will be outlined in the relevant Section 22a Collaboration Agreement.

9.2 The Constabularies recognise the sensitivity of the personal information they hold and its duties in respect of such data to protect individuals from the threat of:

- The use of incorrect information,
- The misuse of correct information, and
- The unauthorised loss or disclosure of their information.

9.3 The Constabularies recognise and ensure their Data Protection practices are in line with the Authorised Professional Practice (APP) on Data Protection.

9.4 Data Protection advice is provided to the Constabularies by the Data Protection Team, Information Compliance Unit.

9.5 This Policy is supported by the Data Protection Policy

10. Data Quality

10.1 Norfolk and Suffolk Constabularies are committed to managing information successfully and ensuring that all information is recorded properly at the outset to ensure the principles of the Data Protection Act 1998 are followed, which require personal information to be:

- adequate, relevant and not excessive,
- accurate, relevant and up to date, and
- kept for no longer than is necessary for its purpose.

10.2 In addition, it recognises that data quality is integral to effective policing by ensuring that accurate and up to date information is available, when it is

[2] http://www.app.college.police.uk/app-content/information-management/?s=

needed to those that need it. Failing to achieve an appropriate level of quality for Force information can present operational problems, for example failing to identify a vital link between records, making a false arrest, executing a warrant at the wrong address or making an inappropriate or misleading disclosure. It can also have legal implications in terms of failing to comply with the Data Protection Act 1998, Human Rights Act 1998, Freedom of Information Act 2000 and may leave each Force vulnerable to civil litigation over the use of incorrect information, enforcement action by the Information Commissioner and/or a monetary penalty up to £500,000.

10.3 Information Asset Owners have responsibility for ongoing monitoring of the quality of data within their area of business, to ensure it is properly obtained, held, used and disclosed.

10.4 Data Quality advice is provided to the Constabularies by the Audit Officer, Information Compliance Officer - Information Compliance Unit and the Records Manager, Records Management Unit.

10.5 This Policy is supported by the Data Quality Policy.

11. Audit and Monitoring

11.1 To support Information Asset Owners, further independent audits are undertaken by the Information Compliance Unit in the form of an Annual Strategic Audit Plan which selects from the information assets presenting the highest risk to the constabularies. The nature and scope of audits takes into account the risks, resources available, the changing environment and national requirement.

11.2 The audit process will reflect the process laid down in the College of policing Authoirised Professional Practice - https://www.app.college.police.uk/app-content/information-management/data-protection/audit/#risk-assessment-process

11.3 A number of transaction monitoring audits are also conducted by the Information Compliance Unit to test compliance with force policies and procedures.

11.4 Audit and monitoring advice is provided to the Constabularies by the Audit Officer, Information Compliance Unit.

11.5 This Policy is supported by the Audit and Monitoring Procedure.

12. Information Security

12.1 Norfolk and Suffolk Constabularies are committed to delivering compliance with the seventh Data Protection Principle which requires organisations to ensure appropriate security measures are in place in order to protect the personal information which it holds.

12.2 The Constabularies recognise the distress, damage and harm which may be caused to individuals should information about them be lost, inappropriately destroyed, disclosed or accessed.

12.3 The Constabularies will ensure that its information is afforded adequate protection, commensurate with its value and the risks associated with its potential loss or compromise.

12.4 The Constabularies will apply practical risk assessment management methodologies and processes through:

- Managing its information securely by application of the ACPO/ACPOS Information Systems Community Security Policy.
- Demonstrating standards of assurance that allows secure connection to national police systems in line with the ACPO/ACPOs Accreditation Policy for National Police Systems, and
- Ensuring that a process is in place to report information security incidents and other information risk issues through the Security Incident Reporting Procedures and escalate as appropriate for professional advice and/or remedial action.

12.5 The creation of an Information Risk Management Policy and Force Risk Appetite Statement which will delegate certain levels of risk based decisions associated with certain information assets to Information Assets Owners and Information management practitioners.

12.6 Information Security advice is provided to the Constabularies by the Information Security Unit.

12.7 This Policy is supported by the Information Security Policy, Information Risks Management Policy and Force Risk Appetite Statement.

13. Records Management

13.1 Norfolk and Suffolk Constabularies are committed to improving records management to ensure that information is managed throughout its life cycle in a systematic, cost-effective and efficient manner. In particular, it provides a means of applying controls to information to maintain its evidential weight and ensure its authenticity, availability and integrity.

13.2 Good practice in records management ensures that information in any format is readily available for policing use including sharing with partner agencies where necessary.

13.3 Records Management, through the proper control of the storage and volume of records, reduces the cost in finding and managing information, and promotes best value in terms of human and space resources.

13.4 Records Management advice is provided to the Constabularies by the Records Management Unit.

13.5 This Policy is supported by the Records Management Policy and Review, Retention and Disposal Procedures & Schedules.

14. Freedom of Information Act 2000

14.1 Norfolk and Suffolk Constabularies are committed to adopting an open and transparent approach in relation to policing. It is cognisant of its statutory duties and will work towards proactive publication of information as far as is possible without compromising policing purposes in compliance with the Freedom of Information Act 2000. FOIA)

14.2 Requests for information made under the FOIA will be processed in accordance with the ACPO Manual of Guidance for the FOIA.

14.3 To manage the risk of harm to individuals which could be associated with the disclosure of information under FOIA, consultation will take place with National leads, Business Owners, Chief Officers and Communications Department staff as necessary.

14.4 Freedom of Information advice is provided to the Constabularies and public by the Freedom of Information Team, Information Compliance Unit.

14.5 This Policy is supported by the Freedom of Information Policy.

15. Information Sharing

15.1 Norfolk and Suffolk Constabularies are committed to sharing information with other agencies where necessary for the prevention or detection of crime or the apprehension or prosecution of offenders or where there is a lawful basis for the personal information to be shared with another agency to enable that agency to carry out their statutory responsibilities.

15.2 The sharing of police information is carried out with regard to the APP for information management and governed through the creation of information sharing agreements, protocol and/or Memorandums of understanding which can be justified in law, securely undertaken and are auditable.

15.3 A central record of all Information Sharing Agreements will be maintained and made available to Constabulary personnel.

15.4 Information Sharing advice is provided to the Constabularies and its partners by the Information Sharing Officer, Information Compliance Unit.

15.5 This Policy is supported by the Information Sharing Policy.

16. Disclosure of information

16.1 Norfolk and Suffolk Constabularies are committed to building safer communities by working with local partners and engaging in multi-agency working. Where requests for information are made this should identify a suitable legal gateway and / or policing purposes – in most cases this means that the request for the information will be made under a statute. Where no legal gateway exists, the requestor should identify a statutory obligation which cannot be achieved without the disclosure of information. In these cases, the Constabularies will disclose the information if this does not impact upon any current policing process.

16.2 If an officer identifies a risk to individuals during an investigation and believes it is necessary to proactively disclose information over and above the routine disclosures made as part of a police investigation, and this disclosure will have a significant impact upon the person under investigation (such as to the employer) this risk assessment process should be used and authorisation gained from an officer of ACPO rank – unless the delay caused by such a process would cause harm or a further crime to be committed.

16.3 Disclosure advice is provided by the Information Compliance Manager and Data Protection Decision Makers/Assistants.

16.4 This Policy is supported by the Information Sharing Policy, Disclosure and Barring Policy and Common Law Police Disclosure Policy.

17. Information Compliance and Handling Information Disputes

17.1 Norfolk and Suffolk Constabularies are committed to ensuring that information assets are created with information compliance considerations fully engaged and that privacy considerations are identified at the outset of projects, initiative and system design stages through the use of Privacy Impact Assessments.

17.2 A central (Joint) Information Asset Register will be maintained by the Compliance Officer and made available (where necessary) to constabulary personnel and the public. This will clearly distinguish the purpose of the asset and Information Asset Owner.

17.3 Norfolk and Suffolk Constabularies are committed to ensuring that those who exercise their statutory information rights and challenge the manner in which constabulary information is managed, are treated in a fair and lawful manner. Information disputes and challenges arising from data retention, handling etc. will be administered by the Information Compliance Officer, Information Compliance Unit.

17.4 This policy is supported by the Requests for removal of DNA, Fingerprints and PNC information and Data Protection Policy.

18. Information Management Training

18.1 Norfolk and Suffolk Constabularies are committed to ensuring their staff are fully informed of their information management responsibilities in the form of:

- NCALT training in respect of:
  - Data Protection,
  - Freedom of Information,
  - Information Security,
  - Government Protective Marking, and
  - MoPI.
- Classroom training:
  - New recruits,
  - Ad hoc sessions.
- Regular forcewide announcements and news articles.
- Information Asset Owner Training.

18.2 This Policy is supported by the Information Management Training Procedure.

19. Who to Contact about this Policy

19.1 Questions regarding this policy and its operation should initially be referred to your Force Information Management Team:

- Suffolk Constabulary, Police Headquarters, Martlesham Heath, Ipswich, IP5 3QS. Tel 01473 613500
- Norfolk Constabulary, Operations and Communications Centre, Jubilee House, Falconers Close, Wymondham, Norfolk, NR18 0WW.