INFORMATION MANAGEMENT

Owning Department: Information Management / Assistant Chief Officers

Department SPOC: Information Management Dept Managers

Risk Rating: Medium High

Legal Sign Off: 30/06/2023

JNCC: September 2023

Published Date: 04/09/2023 (v1.1)

Review Date: 03/09/2026

Index

Legal Basis

Legislation specific to the subject of this policy document:

- Common law duty of confidentiality

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

- Human Rights Act 1998 (in particular A.14 – Prohibition of discrimination)
- Equality Act 2010
- Crime and Disorder Act 1998
- Health and Safety at Work etc. Act 1974 and associated Regulations
- General Data Protection Regulation (GDPR) and Data Protection Act 2018
- Freedom Of Information Act 2000
- The Civil Contingencies Act 2004
- Bribery Act 2010
- 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 documentation which you must check this document against:

- College of Policing – Code of Ethics
- Norfolk and Suffolk Constabularies' Standards of Professional Behaviour
- College of Policing – Authorised Professional Practice
- Information Management Policy
- Data Protection Policy
- Freedom of Information Policy
- Information and Cyber Security Policy and Procedure
- Records Management Policy
- Information Sharing Policy
- Information Risk Management Policy and Procedure
- Information Asset Owners Policy
- Information Management Risk Appetite Statement
- Data Quality Policy
- Data Protection Impact Assessment Policy
- Information Audit and Monitoring Procedure
- Information Asset Owners Guide
- Disclosure and Barring Service Policy
- Common Law Police Disclosure Policy
- Requests for Deletion of Records from National Police Systems Policy
- Information Management Training Procedure
- Information Commissioner's Office Guidance
- College of Policing APP: Freedom of Information
- NPCC Data Protection Manual of Guidance
- 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. Introduction

1.1 Information is critical to every part of policing, and it is key that Norfolk and Suffolk Constabularies ('the Constabularies') enhance the focus on the information that is captured, used, held, shared, managed and disposed of to maximise operational effectiveness and minimise risk and non-compliance.

1.2 The Constabularies recognise that the collection of appropriate information with a high standard of data quality, its accurate assessment and timely exploitation are core to delivering efficient and effective policing.

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

2. Aims

2.1 This policy aims to support the 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.

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

2.3 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 and standards of compliance.

3. Statement of Policy

3.1 This policy has been formally agreed via the approved policy development/review process. It will be maintained by the Information Management Department in conjunction with the Central Policy Unit.

3.2 The policy is intended to promote equality, eliminate unlawful discrimination and actively promote good relations regardless of age, disability, gender reassignment, marriage or civil partnership, pregnancy and maternity, race, religion or belief, sex, sexual orientation, economic or family status.

3.3 Managers have a responsibility to ensure this policy is applied fairly, and unless otherwise stated, all policies and procedures are non-contractual.

4. Applicability

4.1 This policy applies to all information held and used by Norfolk and Suffolk Constabularies including that which falls under the General Data Protection Regulation (GDPR) and Part 2 of the Data Protection Act 2018, such as data processed for administrative purposes, HR, Finance, fleet, estates etc. and data which falls under the Part 3 provisions of the Data Protection Act 2018 which transposes into law the data processed for law enforcement purposes.

4.2 This policy applies to Norfolk and Suffolk Constabularies' 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.

4.3 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.

5. Information Management Governance

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

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

- Chairing the Information Management Steering Group (IMSG);
- Oversight of this policy through the IMSG;
- Setting the Constabularies' (Local) Information Management 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; and
- Advising the Chief Constables 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.

5.3 The **Information Management Steering Group (IMSG)** meets approximately every six weeks, for which, terms of reference exist.

5.4 Compliance and Data Protection Officer holds the role of designated force Data Protection Officer.

5.5 An Information Management Department will be structured to allow effective dialogue on information management (including data protection issues) between the Chief Officers, Data Protection Officers and other

relevant staff. The department will be structured to support the duties of the Data Protection Officer in a timely manner. The following areas fall under Information Management: Data Protection, Freedom of Information, Records Management, Information Security, Information Sharing, Information Compliance, Disclosure and Barring (including common law police disclosures).

5.6 **Information Asset Owners** are appointed and 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.

6. Information Management Strategy (IMS)

6.1 A Force Information Management Strategy is produced and maintained under the direction of the Assistant Chief Officers.

6.2 The Information Management Strategy (IMS) will set out principles to:

- Improve data quality.
- Support efficient and effective operational service delivery.
- Improve decision making and policy development.
- Ensure compliance with legislation.
- Reduce levels of information related risk and ensure that information is protected and secure.
- Provide confidence and assurance to the Senior Information Risk Owner (SIRO) on effective information risk management.
- Retrieve information quickly and easily and make it available when required.
- Know what to keep and what to dispose of and when – removing duplication and the “keep it just in case” approach.
- Ensure that good information rights practice is embedded into the culture and day to day processes of the service and into emerging technologies and systems, therefore improving public confidence.

7. Use of Information

7.1 All Information held by the 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.

7.2 There is an expectation of trust on individuals to handle the Constabularies' information appropriately and with due care and diligence.

7.3 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 complaint/misconduct/discipline enquiry or through the progression of an investigation.

7.4 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.***

Information Charter and Fair Processing Notices

7.5 An Information Charter will be produced and published on the Constabularies' websites and fair processing notices will be developed to ensure openness and transparency in the use of the constabularies' data.

8. Information Management Areas of Business

8.1 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

9. Management of Police Information (MoPI)

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

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

10. GDPR and the Data Protection Act 2018

10.1 The 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 GDPR and Data Protection Act 2018. They will endeavour to ensure that the data protection principles are applied to all personal information held and used by both the constabularies.

10.2 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.

10.3 The Compliance and Data Protection Officer is the designated Data Protection Officer for both Norfolk and Suffolk Constabularies.

10.4 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.

10.5 The Constabularies recognise and ensure their Data Protection practices are in line with the Authorised Professional Practice (APP) on Data Protection and the National Police Chief's Council Data Protection Manual of Guidance.

10.6 Data Protection advice is provided to the Constabularies by the Data Protection Officer and nominated staff.

10.7 This policy is supported by the Data Protection Policy.

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

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

11. Data Quality

11.1 The Constabularies are committed to managing information successfully and ensuring that all information is recorded properly at the outset to ensure the principles of the GDPR and Data Protection Act 2018 are followed, which require personal information to be:

- adequate, relevant and limited to what is necessary,
- accurate, where necessary kept up to date,
- erased or rectified without delay where inaccuracies are identified, and
- kept no longer than necessary with appropriate time limits established to enable review of retention periods.

11.2 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 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 GDPR, Data Protection Act 2018, 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 a maximum of £17million.

11.3 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.

11.4 Data Quality advice is provided to the Constabularies by the Data Protection Officer, Senior Records and Data Quality Manager and Records and Data Quality Manager and key information management practitioners including, Audit staff, Information Compliance staff and Records Management staff.

11.5 This policy is supported by the Data Quality Policy.

12. Audit and Monitoring

12.1 To support Information Asset Owners, further independent audits are undertaken by the Audit and Compliance function of the Information Management Department, who undertake an Annual Strategic Risk Assessment and 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.

12.2 The audit process will reflect the process laid down in the College of Policing Authorised Professional Practice - Information management | College of Policing and can be subject to change by the IMSG priorities.

12.3 A number of daily transaction monitoring audits are also conducted by the Audit and Compliance function to test compliance with Force policies and procedures.

12.4 Audit and monitoring advice is provided to the Constabularies by the Audit and Compliance Function.

13. Information Security

13.1 The Constabularies are committed to delivering compliance with the Data Protection Security Principle which requires organisations to process information in a manner that ensures appropriate security to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

13.2 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.

13.3 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.

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

- Managing its information securely by application of the Community Security Policy.
- Demonstrating standards of assurance that allows secure connection to national police systems in line with the 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.

13.5 The Information Risk Management Policy and Force Information Management Risk Appetite Statement delegates certain levels of risk-based decisions associated with certain information assets to Information Assets Owners and Information management practitioners.

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

13.7 This policy is supported by the Information and Cyber Security Policy and Procedure, Information Risk Management Policy and its accompanying

Local Force Information Risk Appetite Procedure as well as the Information Management Risk Appetite Statement.

14. Records Management

14.1 The 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.

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

14.3 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.

14.4 Records Management advice is provided to the Constabularies by the Records Management and Data Quality Department.

14.5 This policy is supported by the Records Management Policy and Review, Retention and Disposal Policies (crime related and non-crime related) and Schedule.

15. Freedom of Information Act 2000

15.1 The 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).

15.2 Requests for information made under the FOIA will be processed in accordance with the College of Policing APP: Freedom of Information.

15.3 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.

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

15.5 This policy is supported by the Freedom of Information policy.

16. Information Sharing

16.1 The 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.

16.2 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.

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

16.4 Information Sharing advice is provided to the Constabularies and its partners by the Information Sharing Officer.

16.5 This policy is supported by the Information Sharing policy.

17. Disclosure of information

17.1 The 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.

17.2 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 a Chief Officer – unless the delay caused by such a process would cause harm or a further crime to be committed.

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

17.4 This policy is supported by the Information Sharing policy, Disclosure and Barring Service policy and Common Law Police Disclosure policy.

18. Information Compliance and Handling Information Disputes

18.1 The 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, initiatives and system design stages through the use of Data Protection Impact Assessments.

18.2 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.

18.3 The Constabularies are committed to ensuring that those who exercise their statutory information rights and challenge the manner in which constabularies' 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 function.

18.4 This policy is supported by the Requests for Deletion of Records from National Police Systems policy.

19. Information Management Training

19.1 The Constabularies are committed to ensuring their officers and staff are fully informed of their information management responsibilities in the form of:

- MLE training in respect of:
  - Managing Information,
  - Freedom of Information,
  - Information Security,
  - Government Security Marking, and
  - MoPI.
- Classroom training:
  - New recruits,
  - Ad hoc sessions.
- Regular force wide announcements and news articles.
- Information Asset Owner training.

19.2 This policy is supported by the Information Management Training Procedure *(being drafted)*.

20. Who to Contact about this Policy

20.1 Questions regarding this policy and its operation should initially be referred to the Information Management Team:

- Compliance@suffolk.police.uk
- Informationsecurity@suffolk.police.uk
- MoPIAnalysts@suffolk.police.uk