CLEVELAND POLICE

Information Management Policy

Policy Number	320
Policy Owner	Director of Standards and Ethics
Version	1.1
Last Review Date	August 2020
Next Review Date	August 2022
Date of approval	16th April 2019
Protective Marking	Official

This document has been assessed for:	
Compliance with Legislation	☒
Equality Impact Assessment	Not required
Freedom of Information issues	☒
Human Rights compliance	☒
Health and Safety	☒
Risk Management	☒

Information Management Policy

1. Policy statement

Information is the lifeblood of policing; it underpins our operational activities, processes and systems. It leads to effective investigations, timely arrests and appropriate criminal justice outcomes. It also helps to prevent further crimes being committed and is vital in the fight against crime.

Information Management describes the means by which an organisation efficiently plans, collects, organises, uses, controls, shares, disseminates and disposes of its information, and through which it ensures that the value of that information is identified and exploited to the fullest extent.

2. Purpose

The aim of this policy is to ensure that all Force information is held lawfully and is readily accessible on demand; promote consistent management of all records throughout their lifecycle; ensure all information is captured and maintained in such a way that its evidential weight and integrity is not compromised; promote auditable decision-making and to maintain information management best practice.

This policy applies to everyone with access to the Force's information, whether employees, contractors, volunteers, professional partners and employees of other organisations, and whether on police or partner premises, or working remotely.

The policy applies to all information, whether held digitally or on paper or other physical format. This includes (but is not limited to) text, data, images, and voice and video recordings, and covers both structured material (e.g. Force IT systems and databases) and unstructured material (e.g. documents, emails).

Records are documents or data that provide evidence of the Force's actions and decisions and are required for legislative and audit purposes, as well as providing an 'organisational memory'. Generally the same principles contained within this policy should be taken as applying to both information and records.

The policy applies to both personal and non-personal information and covers all information gathered for the effective running of the organisation. This includes information required for 'law enforcement purposes', which is defined by the Data Protection Act 2018 as:

- "The law enforcement purposes" are the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

The law enforcement purposes provide the legal basis for the collecting, recording, evaluating, sharing and retaining of police information.

3. Principles

The key information management principles are as follows:

Responsibility - Information management is everyone's responsibility and they must ensure that information is used appropriately and in accordance with the Force Values and Behaviours, Code of Ethics and the Data Protection Act 2018 incorporating GDPR.

Accessibility and re-use - All information obtained or created for organisational or policing purposes belongs to Cleveland Police. It must be treated as an organisational asset, and managed and stored in an authorised system and/or location.

Wherever feasible, information should be recorded only once and all policing information concerning an individual (also referred to as 'a nominal') should be linked so that it is easily retrievable.

All information should be in a form which facilitates re-use and interoperability across the Force and with other forces where appropriate.

Wherever feasible, information should be migrated to newer formats and/or systems when the current ones become obsolete.

Quality - All information should be accurate, adequate, relevant and timely, and recorded in a manner appropriate for potential future disclosure, and in accordance with national and legal requirements.

In regard to information held for a policing purpose, the information should comply with the principles of the National Intelligence Model (NIM), and should be evaluated, graded and recorded accordingly. Where appropriate, the source of the information, the nature of the source, any assessment of the reliability of the source, and any necessary restrictions on the use to be made of the information will be recorded to facilitate later review, reassessment and audit.

Data quality audits and data improvement initiatives will be carried out where appropriate.

Quantity - The quantity of any information, especially personal information, that is captured and retained should be proportionate to the law enforcement purpose or business requirement.

Security - Safeguards to the information held by the Force will be provided through the Information Security Policy, and through compliance with other policies, standards and guidance.

Appropriate safeguards must be put in place to protect personal, sensitive and/or information classified under the Government Protective Marking Scheme (GPMS) or Government Classification Scheme (GCS). The extent of the safeguards should be in proportion to the degree of risk posed.

Disclosure - The ethos of MOPI is that information should be re-used in order to fulfil a law enforcement purpose and/or to protect the public from harm. However, the Force is also required to comply with the law and therefore information may only be

accessed, shared or disclosed internally or externally when it is considered appropriate to do so.

Particular care should be taken with personal, sensitive and/or information classified under the GPMS / GCS to ensure sharing is lawful and proportionate. Information Sharing Agreements (ISAs) should be put in place where personal data is being regularly disclosed to or received from partners, and Data Processing Agreements (DPAs) drawn up where one party is processing information on another party's behalf.

Transparency - It is the Force's policy to fully comply with the Freedom of Information Act 2000. Information which is not exempt from disclosure will be made available on request.

Retention - All information, particularly personal data, should not be retained longer than necessary. Information obtained for law enforcement purposes will be reviewed, retained and disposed of on a risk assessment basis, and in accordance with the APP on Information Management, wherever practical. In all other cases, time-based disposals will be applied, in accordance with the Cleveland Police Retention Schedule.

Risk Management -Information management risks will be considered, and appropriate mitigations implemented, whenever significant changes are made to Force processes or systems. Where personal data is being processed, this will require the completion of a Data Protection Impact Assessment; see Cleveland DPIA Policy.

4. Powers and Legislation

This policy is underpinned by:

- The UK Data protection Act 2018 incorporating GDPR
- The Human Rights Act 1998
- The Freedom of Information Act 2000
- The Computer Misuse Act 1990
- College of Policing Authorised Professional Practice on Information Management
- Management of Police Information

5. Policy Detail

Cleveland Police has a duty to obtain, use and proactively share a wide variety of information with our partners, in order to discharge our collective duties effectively and keep communities safe. The collection, exploitation and sharing of information is an essential function of policing. Managing information effectively is crucial for:

- Keeping people safe
- Providing evidence to investigate, prosecute and prevent crime
- Managing the business
- Mitigating risks around the poor use of information such as non-compliance with legislation, harm to the public and loss of reputation

It will ensure that all staff, including our partners, understand their responsibilities with information and are provided with the knowledge and standards to use that knowledge in line with legislative requirements and in pursuance of our policing vision and aims.

The Information Management Policy with supporting guidance will set out how Cleveland Police will ensure that information is managed effectively and lawfully throughout its lifecycle.

This policy is intended to provide officers, staff, contractors, volunteers and other relevant parties with clear and concise guidance that enables them to create, use, retain and dispose of information appropriately, lawfully and with confidence.

This policy is intended to enable consistent and transferable procedures and information sharing across other police, government and partnership organisations.

The Chief Constable has a responsibility under the Management of Police Information (MOPI) Code of Practice to establish and maintain an Information Management Strategy (IMS) under the direction of an officer of NPCC rank or equivalent. This policy and supporting guidance cover the key points of an IMS as defined by the Authorised Professional Practice (APP) on Information Management and is therefore intended to fulfil that requirement.

6. Roles and Responsibility

Chief Constable - Overall responsibility for Information Management rests with the Chief Constable as Data Controller for the Force. The Data Protection Act 2018 places a legal obligation[1] on the Chief Constable, as Data Controller, to comply with the data protection principles, subject to exemptions, in relation to all personal information processed by the force.

Senior Information Risk Owner - The Senior Information Risk Owner (SIRO) holds responsibility for overseeing all central functions for Information Management and for making strategic decisions in regard to information risks across Cleveland Police, particularly when there is a potential conflict between operational and security requirements.

Data Protection Officer – The Data Protection Officer, DPO, is now a statutory role within Cleveland police. The full role of the DPO is defined in Article 39 of the Act, located at Appendix A. To summarise they are responsible for ensuring the Force is meeting their obligations under the Data Protection Act 2018 which incorporates the General Data Protection Regulation, GDPR and the Law Enforcement Directive.

Head of Information Management -The Head of Information Management (also the statutory DPO for the Force), manages the statutory "right of access" functions, Freedom of Information, Information Rights and Disclosure and Barring Service, DBS. Also ensures the core elements which create the foundations for efficient information management are being implemented and managed force wide. These being:

- Compliance

[1] Article 5(2) of the GDPR - "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 [the other data protection principles]"

- Quality
- Efficiency
- Security
- Sharing

Information Asset Owners - Information asset owners[2] (IAOs) are responsible for the management and security of paper information and electronic data that is processed, handled, stored, disseminated (information sharing) and destroyed by their respective business areas. IAOs are also responsible for agreeing system downtime with ICT so that servers can be patched against known vulnerabilities.

Information Security Manager -The Information Security Manager provides advice and guidance to the Force on all aspects of information security. This includes conducting risk analyses and specifying appropriate controls to preserve the confidentiality, integrity and availability of Force systems and processes. The role also involves responding to information security incidents, providing day-to-day advice to staff, supporting the specification and commissioning of and changes to systems, and engaging with national bodies regarding information assurance.

Records Manager – The Records Manager coordinates and where appropriate leads on force compliance with its statutory and regulatory responsibilities in relation to the retention, review and deletion of Force records. Identifies and eradicates duplication within the Forces crime management systems, predominantly NICHE.

Data Protection/GDPR Auditor – The DPA/GDPR Auditor assesses and provides assurance against compliance with DPA/GDPR.

Data Steward(s) - The role of a Data Steward is specifically tasked with maintaining data control in data governance and master data management initiatives on a day-to-day basis. Data Stewardship is required for data implementation and data management to succeed. Although not referred to as Data Stewards the Force does have a number of roles which complete some of the tasks of a Data Steward, these include Quality and Assurance Officers who undertake regular and comprehensive quality control checks in order to ensure crime, incident reports and other documents contain all relevant information and comply with relevant standards and the Data Quality Clerks who review and merge duplicate records within NICHE. **IAO should review their area of business to identity in there is a need for more Data Stewards.**

Managers and Supervisors - Managers and supervisors have the responsibility to ensure their staff are aware of and adhere to policies and procedures relating to information management and the appropriate use of information systems. They are also responsible for identifying any local risks relating to information and escalating them if appropriate, in accordance with the Information Security Policy.

All Staff - All those who access and use Force information are responsible and accountable for the information they handle whether on computers, on paper, or through the spoken word. Data Protection training is mandated for all and must be completed every other year via an on line NCALT training package.

---

2 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/706951/Guidance_on_the_IAO_Role_-_May_2018.pdf

7. Compliance and monitoring

This policy will undergo regular reviews to assess its effectiveness and applicability; this will be planned at least on an annual basis and may be prompted between planned reviews by any significant changes to legislation or national guidance (APP).

8. Version control

This policy will be reviewed and updated at least every three years by the owner, and more frequently if necessary.

The Corporate Services Department will ensure this document is available on the Force intranet, including any interim updates.

The following identifies all version changes.

Version	Date	Reason for update	Author
0.1	December 2018	New Policy	[redacted]
0.2	Jan 2019	Changed the title of policy owner and amended the review date	[redacted]
0.3	April 2019	Amendment re training	[redacted]
1.0	April 2019	Approved at COG and published	[redacted]
1.1	Aug 2020	Roles and Responsibilities updated	[redacted]