Information Management and Data Protection Policy

Policy Number	320
Policy Owner	Director of Standards and Ethics
Version	2.0
Last Review Date	October 2022
Next Review Date	October 2025
Date of approval	4th October 2022
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 and Data Protection 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 ensures that the value of that information is identified and exploited to the fullest extent.

This policy is underpinned by:

- The Data Protection Act 2018 (DPA) and UK 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

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, cloud based 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.

3. Underpinning Procedures

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 information 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.

3.1 Information Management Principles

The key information management principles are as follows:

3.1.1 Responsibility

Information management is everyone's responsibility and they must be used appropriately and in accordance with the Force Values and Behaviours, Code of Ethics, Police Staff Code of Conduct and the Data Protection Act 2018 incorporating GDPR.

3.1.2 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.

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, also when security of the information is compromised, or significant security risk is identified.

3.1.3 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.

3.1.4 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.

3.1.5 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 Classification Scheme (GCS). The extent of the safeguards should be in proportion to the degree of risk posed.

3.1.6 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 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 Contracts (DPCs) drawn up where one party is processing information on another party's behalf.

3.1.7 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. Exemptions applied will be explained to the requestor.

3.1.8 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.

3.1.9 Risk Management

Information management risks will be considered, and appropriate mitigations implemented, whenever significant changes are made to Force processes, systems, services and business practices involving personal data are implemented. Where personal data is being processed, this will require the completion of a Data Protection Impact Assessment; see Cleveland DPIA Policy. Information risk is identified and managed as per the Risk Management Guidance.

3.2 Data Protection Compliance

Cleveland Police are committed to ensuring our employees handle personal data in compliance with data protection legislative requirements. Namely, the UK GDPR for general for processing, and part 3 of the Data Protection Act 2018 for law enforcement processing defined as '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'.

We do this by ensuring our processing of personal data is in accordance with the data protection principles and adherence to the Information Commissioner's Office's Codes of Practice and Guidance.

Definition of **personal data** – Any information relating to a person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Definition of **processing** – any operation or set of operations which is performed on personal data or on sets of personal data (whether or not by automated means, such as collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, use, disclosure, dissemination, restriction, erasure or destruction).

Definition of **special category** data – relates to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, and the processing of genetic data, biometric data, data concerning health or data concerning a living person's sex life or sexual orientation.

3.2.1 Principles

GDPR principles:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals;

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')

Law Enforcement Principles: (differ slightly to GDPR principles)

Personal data may be contained within any electronic or paper based system including (but not limited to) computer records, email, backups, archives, paper documents, notebooks, CCTV and BWV footage, photos, audio recordings.

3.2.2 Lawful basis for Processing Personal Data

In order to process general personal data under the UK GDPR regime, we must satisfy at least one of the lawful bases:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

In addition when processing any special category data or criminal offence data for general purposes, we must satisfy at least one of the lawful bases determined in GDPR Articles 9 or 10: Special category data | ICO and at least one Schedule 1 condition must be met Data Protection Act 2018 (legislation.gov.uk)

When processing personal for law enforcement purposes, at least one of the following lawful bases must be met.

The processing of personal data for any of the law enforcement purposes is lawful only if and to the extent that it is based on law and either:

(a)the data subject has given consent to the processing for that purpose, or

(b)the processing is necessary for the performance of a task carried out for that purpose by a competent authority.

And when processing special category or 'sensitive' data, at least one condition from Schedule 8 Data Protection Act 2018 (legislation.gov.uk) must be met

The personal data of vulnerable groups, including children should be given extra protection in our policies around the use of their data.

A separate Appropriate Policy Document required by law, exists, for the safeguards when processing special category and sensitive data.

3.2.3 Record of Processing Activity

A record is maintained by Information Management which is reviewed annually by the Data Protection Officer, Data Protection Auditor, Information Asset Owners, Records Manager and Information Security Manager. The Data Protection Audits doubles up as the Record of Processing Activity.

3.2.4 Data Protection by Design

We seek to actively ensure that data protection issues are considered when systems, services, products and business practices involving personal data are implemented, through the Data Protection Impact Assessment process. The ICO must be consulted when any high risks can not be mitigated, the Data Protection Officer will co-ordinate the dialogue.

3.2.5 Managing Data Processors

Cleveland Police endeavour to ensure appropriate protections, including the use of data processing contracts, are in place with any third party organisation who performs Data Processing duties on our behalf. Such Data Processors may be subjected to risk based security and compliance audits.

3.2.6 Training

All employees are required to complete the basic, mandatory information governance training, currently eLearn Managing Information and eLearn Government Security Classifications every 2 years.

Further information governance training will be applicable to roles requiring enhanced levels of training. All information governance training will be document in a Training Needs Analysis matrix. The Data Protection Officer is responsible for identifying information governance training based on roles across the organisation. It is the responsibility of the individual to ensure training is undertaken, with the support from line mangers and Information Asset Owners.

3.2.7 Information Rights

Individuals have rights to request:

- access to their personal data
- rectification of their data
- deletion of their data
- objection to their data being processed
- restriction of their data
- right to data portability

- objection to automated decision making

It is every employee's responsibility to recognise a request, whether made verbally or received in writing, and signpost an individual to send their request to the information.rights.requests@cleveland.police.uk mailbox. Individuals are allowed to make these requests verbally, so all employees must be able to recognise a request and send the request to the mailbox on behalf of the individual immediately, for these requests to be processed within tight statutory timescales.

Likewise, it is every employee's responsibility to recognise a Freedom of Information request. These are not requests for personal data, but instead are information about the organisation which may request performance or financial data from us. Such requests must also be redirected to the Information Rights mailbox.

3.2.8 Privacy Information

Cleveland Police publish privacy notices on the Force website and endeavour to provide privacy information at point of collection and sharing of information, where appropriate.

3.2.9 Consent

When relying on consent as a lawful basis for processing, consent will be sought and managed as per the UK GDPR and Data Protection Act 2018. We will seek informed consent and record where consent is provided. We will refresh consent at appropriate intervals and ensure the uses of the data have not changed from those consented to.

We will make reasonable efforts to check the age of any children giving consent, including the provision of any online services. We will determine whether an individual can provide their own consent, and if not, we will find an effective way to gain and record parental or guardian consent. See Consent Guidance for further information.

3.2.10 Personal Data Breaches

All employees are responsible for notifying the Data Protection Officer and / or Information Security team of a breach or potential breach through the appropriate routes identified in the Information Security Policy. Individuals must do so as soon as they become reasonably aware of a concern, in order for the Data Protection Officer to meet statutory 72 hours window to report applicable breaches to the ICO. Where appropriate, employees should take steps immediately to contain the breach. The Data Protection Officer will assess whether a breach should be reported to the ICO and / or data subjects.

3.2.11 Information Sharing

Cleveland Police fully commit to the lawful sharing of information with partners and others, to benefit society. Information will be shared on a need to know basis, applying the data minimisation principle, anonymising and pseudonymising

wherever possible to safeguard individual's rights. See separate Information Sharing Policy and Data Minimisation, Anonymisation and Pseudonymisation guidance.

4. Other relevant Policies and Procedures

- Appropriate Policy Document
- Information Security Policy
- Data Protection Impact Assessment (DPIA) Policy
- Records Management Policy (in development)
- MOPI APP
- Cleveland Police Retention Schedule
- Information Sharing Policy (in development)
- Data Minimisation, Anonymisation and Pseudonymisation guidance (in development)
- Training Needs Analysis matrix (in development)
- Information Assurance Board Terms of Reference
- Consent guidance (in development)
- ICO codes of practice and guidance - Home | ICO Risk Management Guidance

Departments across the organisation may develop their own operating procedures that may also include data protection compliance elements. These local procedures will be in line with this policy and legislative requirements.

5. Roles and Responsibilities

Chief Constable - Overall responsibility for Information Management rests with the Chief Constable as Data Controller for the Force. The Data Protection Act 2018 and UK GDPR 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) is appointed by the Chief Constable and is responsible 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. The SIRO chairs the Information Assurance Board.

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 GDPR and s71 of the DPA. In summary the DPO is responsible for ensuring the Force is meeting their data protection legislative obligations.

[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]"

Head of Information Management -The Head of Information Management (also the DPO for the Force), manages the statutory "right of access" functions, Freedom of Information, Information Rights, Vetting Unit, Information Security team, Records management and Data Quality team and Disclosure and Barring Service (DBS).

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 compliance with statutory and regulatory responsibilities in relation to the retention, review and deletion of Force records. Identifies and eradicates duplication, promoting data quality within the Forces crime management systems, predominantly NICHE.

Data Protection Auditor – The DP Auditor assesses and provides assurance against compliance with data protection legislation.

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.

Managers and Supervisors - Managers and supervisors are responsible for ensuring 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.

---

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

All Employees and Volunteers - 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, further details will be documented in the Information Governance Training Needs Analysis (under development).

Information Assurance Board (IAB) – The IAB meets quarterly and provides governance and oversight to information assurance. The terms of reference and membership are documented.

Information risk – Information risk is identified and brought to the Information Assurance Board. Risks are formally recorded on the Risk Register for regular review, monitor and action. The Risk and Governance group have oversight of all organisational risk.

6. Appendices

There are no appendices associated with this policy.

7. Compliance and monitoring

The Head of Directorate of Standards and Ethics is responsible for the accuracy and integrity of this document. This policy will be continuously monitored, and updated when appropriate, to ensure full compliance with legislation.

The Head of Directorate of Standards and Ethics will review this process to ensure that all aspects are being adhered to in accordance with the framework of this policy.

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]
2.0	Oct 2022	Policy brought in line with legislative requirements and ICO expectations	[redacted]