College of Policing

college.police.uk

Code of Practice for Law Enforcement Data Service (LEDS)

Subtitle (*Date to be determined*)

Version 0.6 (Draft for consultation)

(*will be*) Presented to Parliament pursuant to Section 39A (5) of the Police Act 1996, as amended by Section 124 of the Anti-social Behaviour, Crime and Policing Act 2014

Draft

CONTENTS

Code of Practice for LEDS **4**

1. Introduction **4**

2 Structure of the Code **5**

3 Policing, Law Enforcement and Safeguarding Purposes **7**

4 Requirements of the Code of Practice **9**

A Securing the data held on LEDS 9

B. Creating the data record on LEDS 14

C. Amending and updating the data record on LEDS 18

D. Validating the data record on LEDS 21

E. Review, Retention and Deletion of data on LEDS 25

F. Accessing and applying the data held on LEDS 29

G. Reporting and analysing the data held on LEDS 32

H. Sharing data held on LEDS 35

I. Accountability for and auditing of LEDS data access and usage 39

J. Training and continuous professional development for LEDS 43

Draft

CODE OF PRACTICE FOR LEDS

1. INTRODUCTION

1.1

This Code of Practice for LEDS provide a framework and operational context for relevant authorities, such as Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) to monitor how LEDS is governed, managed and used. This Code of Practice is intended to provide a robust document with which to hold all LEDS user organisations to account. The existing Codes of Practice for PNC and PND will work in parallel until these systems have been decommissioned, however if information is being accessed through LEDS, organisations and individuals will be expected to comply with the LEDS Code of Practice, and the legislation referenced within the Code. The Codes of Practice for PNC and PND are supplemented by The PNC User Manual and The Police National Database (PND) Manual of Guidance/Business Rules, respectively. These documents will also be referenced as guidance for LEDS until such time as a LEDS User Manual replaces them.

1.2

Everyone in law enforcement and policing, in particular, must maintain high ethical and professional standards when using data and personal information for law enforcement purposes. This is crucial in ensuring public confidence in the legitimacy, confidentiality and integrity of how such data is collected, maintained, managed and applied

1.3

The Code of Practice applies to those who are responsible for developing, maintaining and securing the integrity of LEDS as an information service. It is also applicable to all organisations who are granted access to the platform, through their chief officers, chief executive officers, managers, members and personnel who access the LEDS platform as part of their responsibilities in a law enforcement role and those who will be responsible for training for implementation and use of LEDS. It is the responsibility of each organisation to ensure that all personnel who have access, or may be in a position to gain access are fully aware of the Code and the potential consequences of a breach of the Code. Responsibilities for organisational compliance vest with chief officers (in the case of other organisations using LEDS, their equivalents, Chief Executive Officers, Chief Executives, Directors, Permanent Secretaries and other individuals with senior responsibility for managing the organisation) Whilst they may delegate the execution of those responsibilities to senior

Draft

managers they will be held to account for any failures by the organisation in respect of compliance with the Code.

1.4

The Code of Practice is statutory guidance and is not a technical document. It will be admissible in a court of law and in disciplinary proceedings. The Code will make reference to specific legal requirements such as compliance with the Data Protection Act 2018 or the deletion of DNA profiles and fingerprints under the Police and Criminal Evidence Act 1984 (as amended by the Protection of Freedoms Act 2012) and any breaches of these should be treated in accordance with that legislation. Failing to otherwise comply with the Code may not in itself cause an organisation or individual person to be prosecuted, however the Code, in whole or part, can be used in evidence in any court proceedings. Breaches of the Code in respect of illegitimate or unlawful access or sharing of the information contained with LEDS will be expected to result in disciplinary or legal proceedings for the individuals concerned and may result in dismissal or criminal prosecution.

1.5

The Code of Practice has been designed to be a clear and easily readable document for organisations and users to identify and recognise the expected procedures and practices to be followed in effective use of LEDS, and the desired behaviours for the ethical and lawful application of information sourced through LEDS. LEDS has been developed to encourage data sharing that supports law enforcement and safeguarding purposes and to provide organisations with better opportunities for the use of data in support of operational objectives and priorities. The intention of the Code is to support rather than prohibit data sharing, by highlighting considerations for effective use. The operational benefits of LEDS will be enhanced by following best practice as laid out in the Code.

1.6

Further information on the background to the Code, its statutory status, scope and application can be found in the accompanying Guidance on the Code of Practice for LEDS.

2 STRUCTURE OF THE CODE

2.1

The Code is laid out under sections which reflect data processing functions and supporting functions in managing LEDS as a data platform. Maintaining integrity and quality assurance of the platform are ‘golden threads’ which run through the sections of the Code.

Draft

Data processing is, broadly speaking, the collection, storage and manipulation of items of data to produce meaningful information. Data processing for LEDS may involve various processes or functions, including creating the data record, amending the data record, validating data, reviewing, retaining and deleting data, accessing and applying data, sharing data, analysing data and auditing data. These functions have been broken down within the Code and assigned responsibilities or obligations that describe the good practice for data processing for LEDS. Other supporting functions, such as training for LEDS and securing the data on LEDS have been similarly described.

2.2

Each section includes a short overview which explains the overall requirement in relation to that function. This may include references to specific guidance or legislation which should be read in conjunction with the Code. Guidance on expected performance and practice is issued to police forces from time to time by relevant bodies, such as the National Police Chiefs' Council (NPCC) which succeeded the Association of Chief Police Officers (ACPO) on April 1 2015, and took over ownership of ACPO guidance, which remains current. The College of Policing, the professional body for policing since 2012, is mandated to set standards in professional development, including codes of practice and regulations, for the 43 forces in England and Wales. The College of Policing produces Authorised Professional Practice (APP) which provides further detail to support expectations of good practice. Whilst this in itself does not have statutory mandate, its inclusion within the Code should be considered as a further indication of the standards of practice and performance to be expected of LEDS users. HMICFRS will apply the same standards to all organisations accessing LEDS and will use guidance such as APP as the benchmark of good practice. Whilst written to support policing, wider law enforcement agencies should access APP and should incorporate that guidance into their own context.

2.3

The overview is then followed by a description of the responsibilities or obligations that follow at each level:

The Home Office, currently hosts the NLEDP programme which is developing the platform and will in due course be superseded by a LEDS sustainment organisation. The Home Office will not have statutory responsibility for many of the bodies accessing LEDS but is the owner of the platform. For the purposes of the Code the Home Office is ascribed responsibilities in relation to its role in governance and management of the LEDS platform.

Draft

The National Police Chiefs' Council (NPCC) acts as a co-ordinating body for police forces across the United Kingdom through an agreement made under Section 22A of the Police Act 1996 and has a role in providing leadership and direction to police forces in the United Kingdom who will use LEDS. For the purposes of the Code the NPCC is ascribed responsibilities in relation to the use of LEDS and the access and application of data in LEDS.

The organisation who has been granted access to LEDS, and which may be a police force or other body that has statutory functions to exercise public authority or public powers for any of the law enforcement purposes. This responsibility vests in the chief officer, which term in this code also includes equivalent positions in the case of other organisations using LEDS (Chief Executive Officers, Chief Executives, Directors, Permanent Secretaries and other individuals with senior responsibility for managing the organisation) By default there are also expectations placed upon suppliers of services to adhere to the expectations of the Code in ensuring that the systems which will connect with LEDS facilitate all requirements. LEDS may be accessed by some commercial organisations under data sharing agreements but access is limited to applications which support law enforcement purposes, such as checking for vehicle fraud.

Operational managers within the organisations, who at any level will have some responsibility for managing operation of LEDS access within that organisation, or the performance of personnel (staff or contractors) who may be granted access to the platform. These may occupy a specific LEDS or data role or hold a wider role. Not all the responsibilities outlined will be ascribed to one individual but rather it is assumed there different individuals operating at some level who will assume these responsibilities.

A LEDS user is an individual who has been vetted and approved to log in to the service and trained to access the functionality. They will either be registered as a direct user or will be a member of an organisation which has been granted access through a connecting system. A LEDS user may have a specific designated role such as data entry, or could be a frontline Police Officer accessing LEDS for operational reasons. Therefore some of the responsibilities ascribed under this section will be role specific not generic.

3 Policing, Law Enforcement and Safeguarding Purposes

3.1

Policing purposes are defined in the Code of Practice on The Management of Police Information as:

1. protecting life and property,
2. preserving order,
3. preventing the commission of offences,
4. bringing offenders to justice, and
5. any duty or responsibility of the police arising from common or statute law.

3.2

Law Enforcement purposes are defined under section 31 of the DPA 2018 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."

3.3

This Code addresses both policing, wider law enforcement bodies and other partner agencies using LEDS. For the purposes of clarity, the term ***law enforcement purposes*** is used to encompass the policing purposes as defined above. The Code also addresses wider applications of LEDS data in safeguarding children and vulnerable adults, as ***safeguarding purposes*** which are not included in section 31 DPA 2018.

Draft

4 REQUIREMENTS OF THE CODE OF PRACTICE

A SECURING THE DATA HELD ON LEDS

Requirement

Law enforcement is an increasingly information-led activity. In order that the public can have confidence in the integrity of information on LEDS there must be strict mechanisms for secure storage, restrictions on access and guidance on retention and disposal. LEDS requires robust information assurance structures and processes. Any risk of compromise to data security could lead to the facilitation of crime, issues of public safety, hindrance to investigations, financial loss, damage to the reputations of the data owners, the NPCC and the Home Office. This could impact on the confidence of law enforcement partners and the public. Data security is also reliant on the technical functionality of the systems which exchange information with LEDS.

Why is this relevant?

Data on LEDS will be drawn from a range of sources; local and national police force intelligence, records of crime, reports of missing persons, details of convicted sexual and violent offenders, driver and vehicle records. LEDS will also provide an interface for access with other databases. A number of different vendor systems are used by forces and other law enforcement agencies to house data sources which will connect with LEDS. Each organisation who connects with LEDS will be liable through their chief officer (or equivalent leader) for the efficacy of the systems and their suppliers and the personnel who access and use the data, either directly or indirectly. This responsibility may be delegated to a named individual within the organisation.

Further Suggested Guidance

The Home Office on behalf of the joint controllers for LEDS will provide details of the specific technical and procedural systems requirements. Authorised Professional Practice (APP) on information management has been developed to support the Code of Practice for Management of Police Information (MoPI). APP on Vetting supports the Vetting Code of Practice.

What do you need to do to meet this requirement?

The Home Office is responsible for:

- Applying assurance controls through an accreditation process to ensure that systems which will exchange information with LEDS meet the desired technical and procedural requirements
- Ensuring that the platform has in-built restrictions, such as organisational based access controls (OBAC), attribute based access control (ABAC) or role-based access control (RBAC) or other access security measures to restrict access to unauthorized use of LEDS or unauthorised use of specific data sets within LEDS.
- Applying clearly defined and enforceable joint controller and data sharing agreements to ensure that access to information on LEDS is restricted to organisations which have an identifiable law-enforcement or safeguarding purpose in applying to exchange data with LEDS, who have been subject to an appropriate vetting and due diligence process, and whose access is to data sets is proportionate to what is required in discharging that law enforcement or safeguarding purpose
- Applying clearly defined joint controller and data sharing agreements which stipulate that personnel who access LEDS within both Police and non-police organisations are appropriately vetted (to vetting standards as described by the National Police Chiefs Council 2016) and managed to ensure that individual access to information is proportionate to what is required in discharging a law enforcement or safeguarding purpose
- Applying clearly defined joint controller and data sharing agreements which stipulate the requirements for maintaining data security and the penalties for any organisational breaches of data security

Draft

The National Police Chiefs' Council (NPCC) is responsible for:

- Providing and updating strategic and policy guidance across national and local information systems, to ensure that maintaining security of data is a high priority for all platform users.
- Ensuring that policy and guidance reflect current legislation and regulatory requirements and any changes to be communicated to the relevant organisations in a timely manner

The organisation will be responsible for:

- Nominating a senior manager, a Senior Information Risk Owner (SIRO) or Data Protection Officer (DPO), who is responsible for ensuring that provisions such as the GDPR and Data Protection Act 2018 are adhered to in managing LEDS at the organisational level
- Procuring and maintaining systems that can provide the appropriate technical and security assurance to connect to LEDS. Chief officers will need to provide information and technical assurance to the Home Office which will be reviewed through Government and Information Risk Review (GIRR) process in order to connect to LEDS, and to remain connected. Those which are not deemed suitable will not be approved or may have connection withdrawn if defects, deficiencies, data quality or performance features are not resolved
- Maintaining security of all assets that are used to access LEDS
- Confirming that people who have access to LEDS are appropriately security vetted on appointment, or upon transfer into a role where this becomes necessary. All users of LEDS data must be vetted to the appropriate level to access the information available

Draft

from the platform. The vetting standards for the Police Service are determined by the Vetting Code of Practice 2017 and College of Policing Authorised Professional Practice on Vetting 2019. The vetting standards for non-police organisations will be determined by individual organisational data sharing agreement achieved through either police vetting, or national security vetting (NSV) – designed to protect government assets. Vetting should be renewed at the proscribed intervals as laid out in the College of Policing Authorised Professional Practice on Vetting 2019. Each organisation must nominate a single person who will be responsible for reporting that vetting standards have been implemented and maintained. Organisations that do not follow and maintain stringent vetting procedures may not be approved to connect to LEDS or may have connection withdrawn at a later date.

- Notifying the College of Policing of the status of individual members of forces (Police Officers /Special Constables and Police staff) for whom a Flagstone record should be created or amended in accordance with prescribed timelines
- Ensuring that there is an audit trail for each access event and clear audit processes to support maintenance of data security.

As an operational manager within the organisation you will be responsible for;

- Ensuring that people who access LEDS are fully trained in accordance with the national learning strategy and agreed national standards, are up to date with current practice guidance and fully understand all requirements
- Monitoring the work of those who access data to ensure that access is restricted by role and by relevant purpose.

As a LEDS user you are responsible for;

- Using data access controls responsibly, not sharing passwords or recording passwords in ways which could be intercepted

Draft

- Exercising caution in printing and exporting data from the database. Hard copy data may become out of date or inaccurate and will need to be stored securely, referencing the data and purpose for extraction. Extracted information should be anonymised if it is not necessary to identify personal details. Extracted information should not be retained beyond the application linked to the purpose for abstraction
- Maintaining personal levels of integrity, reporting any changes in personal circumstances, which may affect security clearance or expose to any compromise of integrity. This can include changes in marital status or civil partnership, name or address and financial status, such as a county court judgment or participation in a debt management plan. Failing to do so may result in their vetting clearance being downgraded or withdrawn
- Reporting any suspicious or unusual activity which might suggest malpractice on the part of others.
- Keeping personal knowledge of security requirements up to date by becoming familiar with the Code of Practice, proactively checking for system and legislation updates, reading technical guidance and seeking advice when required.

Management of Police Information (MoPI)

The principles of management of police information (MoPI) provide a way of balancing proportionality and necessity that are at the heart of effective police information management. They also highlight the issues that need to be considered in order to comply with the law and manage risk associated with police information.

A recent decision of the Supreme Court in R (Catt) v Association of Chief Police Officers [2015] emphasises the pivotal importance for police forces in complying with the Code of Practice on the Management of Police Information 2005 and the associated Authorised Professional Practice (APP) on information management.

B. CREATING THE DATA RECORD ON LEDS

Requirement

Data stored in LEDS should have been created or entered for law enforcement or safeguarding purposes. For data to be valid and informative, its structure and meaning needs to be understood by all parties intending to use or handle it. In the context of law enforcement data quality and clarity are an imperative, as there are implications and risks in creating an inaccurate or incomprehensible data record. High quality data will support and inform a decision making process which is auditable and transparent and be capable of being corroborated with other related information. For law enforcement agencies who may be liable for action in response to judgments made upon the information contained within the data it is essential that there is confidence in the accuracy and currency of that information. It is expected that those organisations entering or uploading data onto LEDS will comply with Law Enforcement POLE (Person, Object, Location, Event) Minimum Data Standards.

Why is this relevant?

Having police or law enforcement data on a single accessible data source allows that data to be shared amongst agencies who require it to discharge their law enforcement responsibilities, and they must be confident that the data is fit for purpose. Data on LEDS may be uploaded by bulk transfer or a record may be created or amended by an individual acting on behalf of a Police service or other law enforcement agency. Law enforcement involves many different agencies. Such agencies range from statutory local and national bodies, for example government departments, to charities such as the SSPCA. This will widen with the inclusion of the National Missing Person's Register (NMPR).

Further Suggested Guidance

The Information Commissioner's Office Guide to Law Enforcement Processing. Authorised Professional Practice (APP) on Management of Police Information. ACPO PNC Compliance Strategy (2000) and the Home Office HMIC Report "Police National Computer Data Quality & Timeliness (2001)

What do you need to do to meet this requirement?

The Home Office is responsible for:

- Developing protocols for improving the quality of data on LEDS and proactively leading organisations to put in place measures to ensure that data entered into LEDS as a national asset is accurate and correctly entered
- Monitoring the data quality and providing feedback to inputting organisations.
- Collecting and reporting on data quality in line with LEDS best practice guidance.

The National Police Chiefs' Council (NPCC) is responsible for:

- Providing and updating strategic and policy guidance across national and local information systems, to help data owners understand legal requirements in processing data.
- Providing and updating strategic and policy guidance on the balance between the collection of data that is adequate and relevant for law enforcement purposes whilst able to stand to tests of reasonableness, proportionality and necessity.
- Working with relevant organisations to ensure that minimum data standards are refreshed to reflect changes in regulation and legislation.
- Setting performance standards for timeliness of data entry in business rules or manuals of guidance

Draft

The organisation will be responsible for:

- Confirming that law enforcement data is processed in line with the six law enforcement principles set out under Part 3, Chapter 2 of the Data Protection Act 2018, and that the need to collect personal data for law enforcement purposes can be tested to be reasonable, proportionate and necessary.
- Ensuring that data is entered on to the platform in a timely fashion, and adhering to performance targets set by the NPCC in business rules or manuals of guidance, such as where there is a specific timeliness target in respect of entering details generated by law enforcement events
- Ensuring that there is a systematic process for conducting regular quality checks to confirm that all data is entered accurately, correctly and in accordance with minimum data standards.
- Ensure that monitoring and dip-sampling of the work of those who enter and maintain data is carried out in line with practice guidance on data quality and the results collated and reported
- Ensuring that updating guidance on data quality is disseminated to relevant managers and staff within the organisation to ensure that practice remains valid in line with current national guidelines

As an operational manager within the organisation you will be responsible for;

- Ensuring that individuals who enter data into LEDS have been trained, are up to date with current guidance, and are competent in discharging that role.

Draft

- Monitoring and dip-sampling the work of those who enter and maintain data to ensure information is accurate, relevant and up to date
- Ensuring that updating guidance is disseminated to, and understood by, relevant staff within the organisation to ensure that practice remains valid in line with current national guidelines on data quality and adheres to legislation governing processing of data.

As a LEDS user you are responsible for;

- Ensuring that data that is input to the database is only entered for a lawful purpose and that the law enforcement or safeguarding purpose is specified, explicit and legitimate.
- Ensuring that the data that is entered onto the database is accurate, authentic, adequate, up to date, relevant to the law enforcement purpose, and entered in the appropriate format.
- Recording origin of the information, assessment of the reliability of the information, and any necessary restrictions on the application of the information, to permit later review, reassessment and audit.

Draft

C. AMENDING AND UPDATING THE DATA RECORD ON LEDS

Requirement

Police or law enforcement information must be accurate and up to date while it is being used by agencies who require it to discharge their law enforcement and safeguarding responsibilities, which requires that the data set is proactively reviewed and updated for accuracy and currency. Conversely, if data held on the database is modified to make it inaccurate or incorrect this could interfere with fair and lawful process of justice. Timeliness of entering updating information is critical to make use of the database accurate and relevant. It may be necessary to link information collected for one law enforcement purpose to information collected on LEDS which has been collected for a different purpose. If there are conflicts, errors or duplications between the data sources these need to be resolved.

Why is this relevant?

Law enforcement information comes from various sources and is received in different ways. Within LEDS the originating or 'Responsible Organisation' may share the right to update that information when uploading the data into LEDS, subject to The LEDS Record Update Business Rules. Data that has been entered onto LEDS (or originating databases) should be accurate at the point of entry but new information may arise, for example a missing person may be found or an event may need to be added. This includes arrest, entry into custody, committal (or outcome of) court proceedings. Under the current Victim Code victims are entitled to receive updates within set timescales of between one and five days at key stages in their cases, including when a suspect is arrested bailed or charged. The Information Commissioner has in the past highlighted a concern at the potential effect of poor data on the application of safeguarding checks for pre-employment checks on applicants for sensitive jobs and those involving vulnerable people. Inaccurate or omitted data in such cases could be catastrophic, for example allowing a paedophile to work as a carer or school employee.

Further Suggested Guidance

APP on Management of Police Information provides overall guidance on managing information in a timely and accurate manner. The Code of Practice for Victims of Crime 2006. LEDS Record Update Business Rules.

What do you need to do to meet this requirement?

The Home Office is responsible for:

- Providing and updating strategic and policy guidance across national and local information systems, to help data owners. understand the appropriate protocols for making amendments to the national database

The NPCC is responsible for:

- Setting performance standards for timeliness of data amendment and updating in business rules or manuals of guidance

The organisation will be responsible for:

- Ensuring that there is a systematic process for amending data to maintain accuracy and currency of information
- Ensuring that all data on discontinuance or conclusion of law enforcement proceedings, is entered on to the platform in a timely fashion. For example, in policing there is a specific timelines target in respect of discontinuance or conclusion of law enforcement proceedings following an arrest, report or summons, whereby a minimum of 75 per cent of the total finalisations of each force must be entered onto the LEDS within seven days of the information being received from HM Courts & Tribunals Service (HMCTS)
- Ensure there are procedures in place to rectify errors that are reported by either internal users of the platform, partner agencies or individuals who have sought access to view their data.

Draft

As an operational manager within the organisation you will be responsible for;

- Ensuring that people who amend data held within LEDS have been trained, are up to date with current guidance, and are competent in discharging that role.
- Monitoring and dip-sampling the work of those who enter and maintain data to ensure that information which migrates onto LEDS is accurate, authentic, adequate, up to date, relevant to the law enforcement purpose, and entered in the appropriate format.

As a LEDS user you are responsible for;

- Ensuring that any changes made to data held within the national database are accurate, relevant to the law enforcement purpose, and entered in the appropriate format
- Linking information on an individual who is the subject of an existing record appropriately to the original record and avoiding duplication of entries
- Correcting inaccurate information at the point the inaccuracy is revealed. In ensuring accuracy, it is important not to delete historic information that may be significant (such as details of previous addresses)
- Updating information promptly into the relevant record in accordance with agreed timescales
- Identifying for the audit trail who has augmented the record, when it was changed, for what purpose and on whose instigation if on request.

Draft

D. VALIDATING THE DATA RECORD ON LEDS

Requirement

There are key principles which apply to how data is entered on LEDS, regardless of the originating agency or originating database, regardless of the means by which it enters the national database. Validating police or law enforcement information ensures that all police or law enforcement information is held in accordance with the law and is accurate and up to date before it is shared amongst agencies who require it to discharge their law enforcement responsibilities.

Why is this relevant?

Data validation is the process of ensuring data has undergone a data cleansing process to ensure data quality, i.e. that the currently available data is correct and relevant. For LEDS data validation includes the process of checking LEDS (or originating databases) to ensure that the information gathered from different data sources is clean, accurate and in a standard format. The validation of migrated data for completeness is part of the data migration process for LEDS transferring from one computer storage system to another. This will happen in different ways during the LEDS development stage and will also be an ongoing process, where Police services and other agencies input data through interfaces with existing databases. Data validation can be an automated process. The Information Assets Dashboard is a quality improvement tool created for LEDS to enable data migration and to support organisations in maximising the benefits of LEDS.

Further Suggested Guidance

The Information Commissioners Office Guide to Law Enforcement Processing.

What do you need to do to meet this requirement?

The Home Office is responsible for:

- Proactively leading organisations to put in place measures to ensure that data from existing databases, or inputted directly onto LEDS is entered accurately and correctly
- Collecting and reporting on data quality in line with LEDS best practice guidance

The NPCC is responsible for:

- Providing and updating strategic and policy guidance across national and local information systems, to help data owners understand data requirements before they migrate data.
- Setting performance standards for timeliness of data validation in business rules or manuals of guidance

The organisation will be responsible for:

- Appointing a senior manager, or Data Protection Officer, who is responsible for ensuring that provisions such as the GDPR and Data Protection Act 2018 are adhered to in migrating data into the database.
- Confirming that data is processed in line with the six law enforcement principles set out under Part 3, Chapter 2 of the Data Protection Act 2018, and that the need to collect personal data for law enforcement purposes can be tested to be reasonable, proportionate and necessary

Draft

- Ensuring that there is a systematic process for conducting regular quality checks to confirm that data is entered accurately and correctly
- Ensure there are procedures in place to rectify errors that are discovered during validation procedures
- Ensure that monitoring and dip-sampling of the work of those who enter and maintain data is carried out in line with practice guidance on data quality and the results collated and reported
- Ensuring that updating guidance on data quality is disseminated to relevant managers and staff within the organisation to ensure that practice remains valid in line with current national guidelines.

As an operational manager within the organisation you will be responsible for;

- Ensuring that individuals who validate data entered into LEDS have been trained, are up to date with current guidance, and are competent in discharging that role.
- Monitoring and dip-sampling the work of those who enter and maintain data to ensure that information which migrates onto LEDS is accurate, authentic, adequate, up to date, relevant to the law enforcement purpose, and entered in the appropriate format.

As a LEDS user you are responsible for;

- Ensuring that the data you provide is accurate, authentic, adequate, up to date, relevant to the law enforcement purpose, and entered in the appropriate format.
- Ensuring that the data that is being entered directly into the source system is accurate, authentic, adequate, up to date, and entered in the appropriate format

Draft

Part 3, Chapter 2 of the Data Protection Act 2018 - Six Principles

There are six law enforcement principles in Part 3, Chapter 2 of the Act to follow when processing personal data for law enforcement purposes:

- Processing of personal data for any of the law enforcement purposes must be lawful and fair.
- The law enforcement purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and personal data collected must not be processed in a manner that is incompatible with the purpose for which it was originally collected
- Personal data collected must be adequate, relevant and not excessive
- Personal data processed for any of the law enforcement purposes must be accurate and, where necessary, kept up to date, and every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay
- Personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed.
- Personal data processed for any of the law enforcement purposes must be processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage)..

E. Review, Retention and Deletion of data on LEDS

Requirement

The primary purpose of review, retention and disposal procedures is to ensure the validity and legality of the LEDS data. Reviewing and recording of police information and data is central to risk-based decision making and public protection. To comply with all legal and policy requirements and to protect the integrity of the data on LEDS must be regularly reviewed in order to make informed decisions on retention and deletion, particularly on personal data. The privacy rights of the individual, as enshrined in legislation, should be balanced against the law enforcement requirement. To this end the retention of police information should be determined by the level of risk presented by an individual – this risk must be clearly evidenced and fully auditable if challenged. Data must only be retained proportionately to the law enforcement and safeguarding purposes and must comply with the six law enforcement principles under Part 3, Chapter 2 of the Data Protection Act 2018. It is the responsibility of the data controller for each Responsible Organisation to determine this locally and to ensure any record deletion is reflected on LEDS.

Why is this relevant?

One of the primary functions of LEDS is to ensure that data can be shared appropriately and meaningfully across law enforcement agencies. Elements of the data inputted into LEDS may be retained for longer than other elements to provide both an investigatory and audit thread, subject to Management of Police Information guidance. To balance the law enforcement imperative against data protection principles a regular process for review and deletion of the data should be in place in each organisation. This may be the function of the reviewing officer with delegated responsibility or may partly be discharged by an automated process.

Further Guidance

The Management of Police Information Code of Practice 2005 APP on Management of Police Information with specific reference to the section on Retention, Review and Disposal. The Data Protection Act 2018 Part 3, Chapter 2 of the Data Protection Act 2018.

What do you need to do to meet this requirement?

The Home Office is responsible for:

- Removing or restricting access to data sets where this is not in the public interest.

The NPCC is responsible for:

- Setting and maintaining the policy guidelines for review, retention and deletion of data to ensure that this is conducted in line with current legal requirements
- Promoting compliance to the retention, review and disposal processes
- Working with regulatory bodies to monitor compliance and provide assurance to all organisations
- Agreeing a review process with other data owners to ensure that responsibilities for reviewing and deleting are clearly delineated

The organisation will be responsible for:

- Conducting regular reviews, in accordance with guidance, to ensure that personal data does not remain in the platform beyond a lawful and proportionate period. All participant organisations should either; consistently review the information within LEDS and actively delete information that does not have a proportionate law enforcement purpose, or automatically delete data which meets a set criteria.
- Retaining or deleting personal data according to guidance set by the National Police Chiefs' Council.

Draft

- Ensuring that there is clear guidance available to members of the public as to how (and to what extent) they may exercise individual rights granted under Part 3, Chapter 3 of the DPA 2018 (namely; the right to be informed, the right of access, the right to rectification, the right to erasure or restrict processing, and the right not to be subject to automated decision-making)
- Deleting information that has been shown to be inaccurate, in ways which cannot be dealt with by amending the record
- Deleting other data (vehicle/property/other) which is no longer considered as necessary information for Law Enforcement purposes.
- Deleting biometric data (DNA and fingerprint) in compliance with the circumstances and time frames set in place under of Protection Of Freedoms Act 2012
- Reviewing custody images for deletion should be in line with the Home Office (2017) Review of the Use and Retention of Custody Images

As an operational manager within the organisation you will be responsible for;

- Ensuring that individuals who review data entered into LEDS have been trained, are up to date with current guidance, and are competent in discharging that role.
- Ensuring that the organisational strategy for reviewing records is implemented to ensure such data is used effectively for law enforcement purposes and in compliance with the law
- Ensuring that scheduled reviews in line with guidance associated with the Management of Police Information are carried out within the organisation and that compliance checks are conducted to monitor adherence to the approved retention schedule

Draft

- Responding to any specific requests to review law enforcement information that is being held electronically on LEDS and liaising with ACPO Criminal Records Office (ACRO) where appropriate
- Ensure that LEDS users are applying the data quality principles, good practice when dealing with record management including applying the retention schedule to each action
- Document and record every review undertaken irrespectively of whether it results in any alterations or deletions
- Ensure appropriate records are kept to include what information is stored where allowing the support of the retention and disposal aspects of the procedure
- Following the current review process and ensuring periodic reviews are carried out in accordance with guidance

As a LEDS user (with a reviewer role) you are responsible for;

- Conducting scheduled reviews of data held in LEDS in line with the review periods determined under the MoPI Code of Practice
- Updating the record if any inaccurate information is discovered or if new information is received, this ensures that the record is accurate and up to date
- Ensure data quality principles are adhered to when undertaking initial reviews
- Adhering to the National retention assessment criteria (NRAC) when determining whether policing records should be retained or deleted. This is specific to policing and may not be applicable to other organisations
- Ensure that any data marked for deletion under review is not relevant to any ongoing relevant independent enquiry and should be retained in compliance with the Inquiries Act 2005. It is an offence under that act for a person to destroy or tamper with evidence that may be relevant to an inquiry

Draft

F. ACCESSING AND APPLYING THE DATA HELD ON LEDS

Requirement

The details of individuals and incidents which are recorded on LEDS are an important source of information for application in law enforcement and safeguarding purposes. Data must be applied ethically and in a considered fashion to make justifiable law enforcement decisions, which may be immediate or follow a period of reflection. Among other things decision makers should consider when applying law enforcement information are the objectives of preventing discrimination, promoting good relations and fostering equal opportunities.

Why is this relevant?

Data on LEDS may be used for immediate response to incidents, may be used for operational planning, for investigations, for prosecutions and other law enforcement processes. Data held on LEDS may be accessed to gauge the level of law enforcement response necessary and for an assessment of risk. Some forces have centralised personnel responsible for examining data against other relevant records and informing officers attending incidents of any risks they are likely to face on attending the location or dealing with the subject of the report. This analytical stage involves assessing the situation, including any specific threat or risk of harm. One of the features of LEDS is that officers responding on the frontline will be able to access more data directly.

Further Suggested Guidance

Authorised Professional Practice (APP) on intelligence management is developed and owned by the College of Policing. Police services who are accessing LEDS should adhere to this guidance. Other Law Enforcement Agencies may use this as guidance in developing their own internal standards.

The Home Office is responsible for:

- Working with organisations to ensure that any additional functionality and system developments meet the needs of organisations and users.

The NPCC is responsible for:

- Providing and updating strategic and policy guidance across national and local information systems, to help LEDS users understand the appropriate protocols for applying data obtained through the platform.

The organisation will be responsible for:

- Providing access to training courses for people who analyse or receive data in how to understand, use and incorporate tools such as the National Decision-making Model and National Intelligence Model, critical tools in policing, into law enforcement decision-making processes.

As an operational manager within the organisation you will be responsible for;

- Ensuring that individuals who validate data entered into LEDS have been trained, are up to date with current guidance, and are competent in discharging that role.
- Monitoring the work of those who access LEDS data to ensure that information which informs decision-making is reliable and accurate.

Draft

As a LEDS user you are responsible for;

- Using approved access to LEDS only for purposes which are lawful, proportionate and relevant to a law enforcement task. Accessing LEDS to view the records of individuals for curiosity or profit is a serious breach of data security may result in prosecution
- Understanding and updating knowledge of the capability, application and interrelation of data sets within the platform, to make best use of the available data by correct application appropriate to the law enforcement purpose
- Evaluating the information for provenance, accuracy and reliability proportionately to the purpose of application, for example an immediate incident requires a faster response than accessing information during the course of an investigation
- Applying recognised decision-making tools and risk analysis processes to demonstrate how information has been interpreted, conclusions drawn, recommendations made and predictions made of possible future behaviour
- Recording how the information has been applied for law enforcement purposes, using common terminology and operating principles, that facilitate exchange of information and processing within standard law enforcement systems and to promote common understanding around the certainty or otherwise of any judgements made
- Acknowledging when information is obtained from LEDS (and, where applicable, the originating dataset) assessing and recording judgments on the reliability of the information, and recording any necessary restrictions on the application of the information. This permits later review, reassessment and audit.

Draft

G. Reporting and analysing the data held on LEDS

Requirement

Extracting data is a vital process as data analysis is a particularly important tool in policing and operational law enforcement and safeguarding purposes. Inaccurate data reporting can lead to misinformed strategic decision-making based on erroneous evidence or inefficiencies in applying resources Intelligence-led policing allows police to be proactive rather than reactive. It is used to understand crime and disorder issues and provide insight, clarity and context to support strategic decision making in law enforcement and the tactical deployment of resources. Incorrect analysis could therefore lead to operational errors. Data analysis also identifies effective practice and lessons learnt through a review of tactical and strategic activity.

Why is this relevant?

Data held on LEDS can be analysed to identify patterns in information and to provide statistical data. When reported to strategic decision-makers it enables them to draw inferences so that operational and policy decisions can be made. In policing, intelligence analysts investigate who is committing crimes, how, when, where and why. Analysts produce profiles of crime problems, and produce both strategic (overall, long-term) and tactical (specific, short-term) assessments. This is done at all levels, from local, county, regional and beyond. The more joined up data set within LEDS will enable forces and other organisations to work effectively beyond county lines and across agencies with differing responsibilities.

Further Suggested Guidance

APP on intelligence management is developed and owned by the College of Policing.

What do we need to do to meet this requirement?

The Home Office is responsible for:

- Ensuring that functionality and system developments enable data analytics.

The NPCC is responsible for:

- Providing and updating strategic and policy guidance across national and local information systems, to help data analysts understand the appropriate protocols for applying data obtained through the national database.
- Ensuring that there is clear guidance in the use of decision support tools in policing and the criminal justice system, including algorithmic decision support tools.

The organisation will be responsible for:

- Confirming that people who have an data analytic role are fully trained and competent in discharging that role
- Providing access to training courses for people who analyse or receive data in how to understand, use and incorporate data analytic tools into law enforcement decision-making processes.

As an operational manager within the organisation you will be responsible for;

- Ensuring that people who analyse data held within LEDS have been trained, are up to date with current guidance, and are competent in discharging that role.

Draft

- Monitoring the work of those who analyze and report on data to ensure that information which informs decision-making is reliable and accurate.

As a LEDS user you are responsible for;

- Ensuring that data which is reported is accurate, current and statistically sound.
- Acknowledging when data is obtained LEDS and, where applicable, the originating dataset.
- Applying apply recognised analytical techniques and decision-support systems that provide evidence to demonstrate how information has been interpreted, conclusions drawn, recommendations made and predictions of possible future behaviour have been arrived at.
- Applying the National Intelligence Model (NIM) approach as a Police user to ensure common terminology and operating principles, to promote common understanding around the certainty or otherwise of any judgements.
- Ensuring that information is anonymised where possible when apply data to conduct analysis and there is no justification for identifying specific individuals.

Draft

H. SHARING DATA HELD ON LEDS

Requirement

There are key principles which apply to how data on LEDS may be shared, both amongst law enforcement agencies within the United Kingdom and across borders (across European Union or more widely). Sharing law enforcement information must comply with part 3 of the Data Protection Act 2018 (DPA 2018). The Information Commissioner can issue a monetary penalty for breaches of the DPA 2018 in respect of sharing data overseas, where there is no guarantee of an adequate level of protection for the rights and freedoms of data subjects.

Why is this relevant?

LEDS has been developed so that can be more readily shared amongst agencies who require it to discharge their law enforcement and safeguarding responsibilities. Sharing responsibly will provide accurate and joined-up information in order to bring offenders to justice, to prevent crime and better protect the vulnerable. Organisations will be granted direct or indirect access through data sharing agreements, which will assist accountable sharing and reinforce the principles set out in this Code of Practice. Organisations using LEDS should be confident that the data available complies with the legislative and regulatory frameworks in place and has been ethically captured and appropriate to share. This code assumes two main types of data sharing from LEDS: routine data sharing where data sets are shared between organisations for an established purpose or decisions to share data upon a specific request. Data sharing agreements should cover both aspects. At the time of writing UK law enforcement agencies are also party to the Schengen Information System to share alerts on wanted or missing persons and objects, both inside the EU and at the EU external border.

Further Suggested Guidance

The Information Commissioners Office (ICO) Guide to Law Enforcement Processing and the ICO 2011 Data Sharing Code of Practice. Authorised Professional Practice on Information Sharing which covers sharing police information linked to a policing purpose. The national Information Management Coordination Committee provides guidance to forces in England and Wales. The Wales Accord on the Sharing of Personal Information (WASPI) as applicable to Welsh bodies.

What do you need to do to meet this requirement?

The Home Office is responsible for:

- Creating and upholding data sharing agreements with all organisations which either directly access all functionality on LEDS or will gain access to restricted data sets
- Ensuring organisations are made aware of the human rights records of countries with whom information might be shared, and ensuring organisations have appropriate safeguards to prevent information being used to facilitate human rights abuses especially with countries which participate in, solicit, encourage or condone the use of torture or cruel, inhuman or degrading treatment or punishment for any purpose

The NPCC is responsible for:

- Providing and updating strategic and policy guidance across national and local information systems, to help data owners understand legal requirements in sharing data that is: relevant for law enforcement and safeguarding purposes; appropriate for sharing amongst other law enforcement agencies, appropriate to other specific organisations, and accessible for European and to other overseas jurisdictions

The organisation will be responsible for:

- Creating and upholding enforceable data or information sharing agreements with all organisations which enable the safe and lawful onward sharing of data from LEDS through third party sharing. These must adhere to DPA 2018 principles in respect of processing

Draft

for law enforcement and safeguarding purposes. For policing the drafting of such agreements is subject to a national governance structure, whereby forces must use a national template and follow a local and national consultation process

- Ensuring that updating guidance on data sharing is disseminated to relevant managers and staff within the organisation to ensure that practice remains valid in line with current national and international guidelines
- Ensuring that data that is shared is done so in compliance with legal and policy guidance. For example following the guidance set down by the Information Commissioner's Office on Law Enforcement Processing and ensuring that systems and processes are in place to restrict the sharing of data other than in compliance with legal and national policy guidelines
- Reporting any breach of data privacy by any member of the organisation to the ICO if it is likely to result in a risk to the rights and freedoms of individuals.

As an operational manager within the organisation you will be responsible for;

- Ensuring that processes that enable the safe and lawful sharing of data are followed by personnel with legitimate access to the platform
- Ensuing that there is an audit trail in place for any sharing of data with third party individuals or organisations, including details of the justification for the transfer

As a LEDS user you are responsible for;

- Ensuring that data obtained from the database is only shared for a law enforcement or safeguarding purpose, and that the purpose is specified, explicit and legitimate. Penalties for breaching this requirement result in disciplinary action. As a police user applying

Draft

the national decision model (NDM) and the Police Code of Ethics will help police officers and staff make, examine and challenge decisions whether, or whether or not to share information, when requested directly. If in doubt seek further advice. Examples of data sharing which are not legitimate includes (but is not limited to) the following:

- Sharing information with colleagues in law enforcement for a purpose which is not a specific law enforcement task
- Sharing information with colleagues in law enforcement which is not proportionate or relevant to the identified law enforcement task
- Sharing information externally on individuals who may be in the public eye, whether for profit or for other reasons
- Sharing information externally on individuals, vehicles or other matters to assist third party enquiries (colleagues, family members, friends or others) which are not linked to a legitimate law enforcement purpose
- Sharing information externally to others with a view to perverting the course of justice or interfering with a law enforcement purpose
- Printing, transmitting or exporting data in a manner that could lead to unauthorised access of the information

- Ensuring that, the legitimate transfer of the data, and any necessary restrictions on the use to be made of the information are recorded to permit later review, reassessment and audit of any such data sharing.

Draft

I. ACCOUNTABILITY FOR AND AUDITING OF LEDS DATA ACCESS AND USAGE

Requirement

Accountability is a requirement under the Data Protection Act 2018. To show accountability organisations must evidence that their data protection measures are sufficient. They must have appropriate technical and organisational procedures, which include keeping sufficient records of their processing activities.

Why is this relevant?

An audit is a systematic, independent examination of organisation processes, systems and data to determine whether activities involving the processing, use and sharing of the data are being carried out in accordance with the Data Protection Act 2018, and other expected performance standards such as this Code of Practice or other information compliance standards. Police forces have internal audit procedures and the Home Office maintains a national audit resource which has evolved for the use of PNC. These processes will need to evolve for LEDS. Force often work through Professional Standards departments whose remit might be wider than data and security protection, but find themselves often acting on careless or deliberate breaches of access to data.

Further Guidance

APP on Audit for Data Protection is developed and owned by the College of Policing. Police services who are accessing LEDS should adhere to this guidance. Other Law Enforcement Agencies can access the APP document and use this as guidance in developing their own internal standards. The Home Office (NLEDP) will also provide organisations with some guidance on expected audit practice for LEDS.

What do you need to do to meet this requirement?

The Home Office is responsible for:

- Building into the platform the technical capability for logging access and all relevant processing activity so as to allow those with the responsibility for conducting audit can subsequently make such checks
- Conducting audit checks at a national level, by delegation to the National Systems Audit Team, to proactively drive compliance and support the investigation of malpractice
- Collecting and reporting data on compliance with LEDS best practice guidance, breaches of LEDS (and PNC/PND) integrity and the outcomes of disciplinary procedures

The NPCC is responsible for:

- Providing and updating strategic and policy guidance across national and local information systems, to help data owners mitigate and manage risk in a timely manner
- Proactively leading organisations to put in place measures to protect LEDS as a national asset and mitigate the risk of corruption

The organisation will be responsible for:

- Appointing a senior manager who is responsible for the strategic audit programme and has responsibility for compliance with audit across the organisation

Draft

- Confirming that people who have an identified business need to access the platform in order to carry out their current role are those who have access
- Ensuring that unlawful access or use of information held on the platform can be identified.
- Ensuring that procedures are in place to address and report unlawful access or use of information by individuals who act outside of the Code of Practice
- Ensuring that there is a systematic process for conducting regular audit checks and reviewing audit logs that confirm that access to the Law Enforcement Database is limited to those with authority to access the platform and to ensure such access is both lawful and reasonable.
- Ensure that monitoring and dip-sampling of the work of those who enter and maintain data is carried out in line with practice guidance and the results collated and reported
- Compiling organisational audit reports, including findings and recommendations and action plans detailing how findings and recommendations have been addressed to ensure that any risk has been mitigated
- Providing evidence of regular auditing in accordance with nationally agreed audit standards, together with their outcomes, for external audit and inspection purpose. For example, an inspection by Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS)
- Ensuring that updated guidance is disseminated to relevant managers and staff within the organisation to ensure that practice remains valid in line with current national guidelines.

Draft

As an operational manager within the organisation you will be responsible for;

- Confirming that people who have an identified business need to access the platform in order to carry out their current role are those who have been trained, and records of training and CPD are available
- Confirming that users are adhering to Code of Practice guidance for access and use of data and that records are maintained of their access.
- Monitoring and dip-sampling the work of those who enter and maintain data to ensure information is accurate, relevant and up to date
- Ensuring that updated guidance is disseminated to, and understood by, relevant staff within the organisation to ensure that practice remains valid in line with current national guidelines.

As a LEDS user you are responsible for;

- Complying with all platform access requirements for LEDS set locally within their organisation and nationally
- Ensuring that access to the platform is justified and is only carried out for a lawful purpose
- Ensure that accurate information on justification for a data check is applied upon access
- Retaining evidence or information supporting the validity of LEDS access and processing activity and associated actions for agreed timeframes.

Draft

J. TRAINING AND CONTINUOUS PROFESSIONAL DEVELOPMENT FOR LEDS

Requirement

LEDS is a new system which will be introduced in phased approach. Whilst many of the functions that apply to LEDS are carried over from precursor of feeder data systems LEDS will have a new interface and will require a comprehensive and accessible programme of training upon implementation. Following initial implementation, LEDS users will require updating on system and technical changes as well as refreshing on policy and governance which will evolve as the landscape of law, law enforcement practice, human rights and data protection legislation and guidance also evolves and changes. Training in using LEDS effectively will ensure system integrity, better outcomes for law enforcement, and better protection of individual freedoms.

Why is this relevant?

LEDS is a Law Enforcement Data Service which both exists as a database of information that can be created, amended or deleted in its own right and as an interface to other law enforcement data sources. Police forces will be the main users (by volume) of LEDS, but other law enforcement and partner organisations will also have access. In addition some private sector organisations will also have access; to provide data used by law enforcement and in their commercial operations where there is a legitimate need; say, to prevent or detect fraud.

Further Suggested Guidance

The College of Policing is working with the Home Office to identify the most effective ways to deliver training on LEDS as a new service and to provide guidance on continuous professional development requirements.

What do you need to do to meet this requirement?

The Home Office is responsible for:

- Commissioning and securing training and learning interventions to support the implementation of LEDS as a national data service

The NPCC is responsible for:

- Providing and updating strategic and policy guidance to help organisational data owners understand the appropriate legal technical and best practice requirements in accessing and using LEDS
- Commissioning and securing training and learning interventions to support the continuing application of LEDS as a national data service

The organisation will be responsible for:

- Providing training in accordance with agreed national standards so that staff who carry out data functions on LEDS are fully trained and competent in discharging their role.
- Ensuring that there are performance review processes and continuing professional development opportunities for staff who carry out data functions using LEDS
- Providing staff with updated strategic and policy guidance concerning LEDS data functions and expected operational best practice.
-
-

Draft

- **As an operational manager** within the organisation you will be responsible for;
  - Confirming that people who have an identified business need to carry out data functions on LEDS are fully trained and competent in discharging their role
  - Ensuring that staff who access and use data through LEDS are fully trained in accordance with the national learning strategy and agreed national standards, and competent in using all relevant functionality
  - Ensuring that staff have sufficient time and opportunity for continuous professional development in accessing and using LEDS
  - Ensuring that system and legislation and technical updates are provided to all relevant staff in a timely fashion.

As a LEDS user you are responsible for;

- Keeping personal skills levels up to date by adopting an active continuous professional development approach, accessing refresher training, proactively checking for system and legislation updates and reading technical guidance.

Draft

Requests for information - Freedom of Information and Subject Access Requests

The Freedom of Information Act 2000 (FOIA) provides any person, anywhere in the world the right to access information held by public authorities, subject to a number of exemptions. All police forces are separate public authorities subject to this Act. Guidance from the Information Commissioner's Office (ICO) is available to help organisations meet those responsibilities. The FOIA interfaces with Data Protection Act 2018 (DPA).

FOIA covers information held by public authorities, but not requests for personal information about the person making the request or about another living individual. FOI is about providing access to public information APP on Information Management provides specific guidance on handling such requests in accordance with local policies and procedures.

Data protection legislation protects personal data. Part 3, Chapter 3 of the DPA 2018 provides the following individual rights:

- the right to be informed;
- the right of access (Subject Access Request);
- the right to rectification;
- the right to erasure or restrict processing; and
- the right not to be subject to automated decision-making.

Certain rights under the GDPR, such as the right to object and the right to data portability, do not exist in Part 3 of the Act. Further, there are exemptions and restrictions that can, in some circumstances, be legitimately applied to prevent individuals from exercising rights.

Individuals may exercise the legal right to access information held about them by making a Subject Access Request in writing. In general, verbal requests for information held about an individual are not valid. For policing ACRO Criminal Records Office (ACRO) processes data subject access requests on behalf of most UK police forces by agreement but this is primarily an organisational responsibility.