College of Policing

college.police.uk

Code of Practice for Law Enforcement Data Service (LEDS)

Public Guide

Version 0.4 (Draft for Consultation)

CONTENTS

GUIDE TO THE CODE OF PRACTICE FOR THE LAW ENFORCEMENT DATA SERVICE

1 INTRODUCTION

1.1

This guide provides some background for members of the public or interested parties who wish to understand how the Code of Practice for the Law Enforcement Data Service (LEDS) works to support the integrity of the LEDS system and the management of data. The Code of Practice itself is a separate document *and can be found at xxxxxxxx.*

This guide is intended to provide members of the public, those whose data may be held on LEDS and those interested in the scrutiny of LEDS as a law enforcement asset, with information as to how data could be used within LEDS, and also how to get access to information held about them, or request to change or delete personal material wrongly entered or retained. Also public bodies and Third Sector partner agencies who need to understand how their data will be used if it is provided to LEDS. Private sector agencies who provide data will also want to know how their data is used and what safeguards are in place.

1.2

Data is information that has been translated into a form that is efficient for movement or processing. Data protection is concerned with the fair and responsible use of personal data References to data in the Code include personal data and other factual or intelligence information used for policing and law enforcement purposes.

1.3

The College of Policing, the professional body for Policing in England and Wales has developed the Code of Practice to cover all aspects of the behaviours and use of LEDS and provide a framework for relevant authorities, such as Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) to monitor how LEDS is being governed, managed and used.

1.4

Everyone in law enforcement and the police service, in particular, is expected to maintain high ethical and professional standards when using data and personal information for law

enforcement purposes and so maintain public confidence that data is collected maintained and used legitimately. This Code of Practice should hold all LEDS user organisations to account. Much of the Code is directed at police forces as they will be the main users of LEDS but, as the intention behind LEDS is to provide better access of the information for wider law enforcement and safeguarding purposes, there are other organisations who will fall under the Code.

1.5

The College of Policing, working with the Home Office, wishes to support public confidence in the management and integrity of LEDS by;

a) Supporting the use of LEDS as an effective data sharing platform to promote law enforcement and safeguarding

b) Ensuring the Code of Practice for LEDS provides enough detail for users, managers, suppliers, auditors, and trainers etc. to be clear about their responsibilities in using the system and managing and applying the data within it

c) Providing information within this guidance document as to which bodies will hold the user organisations to account and how to contact them if there are concerns

d) Ensuring that the consequences of breaching the Code are also made explicit.

e) Maintaining the Code of Practice and this Public Guide in a single online publicly available place, so that there is transparency as to how LEDS is governed and managed. Included in that public space will be the answers to frequently asked questions, such as ‘whose data might be held on LEDS?

f) Reviewing and refreshing the Code of Practice and this Public Guide regularly to take account of new developments or thinking.

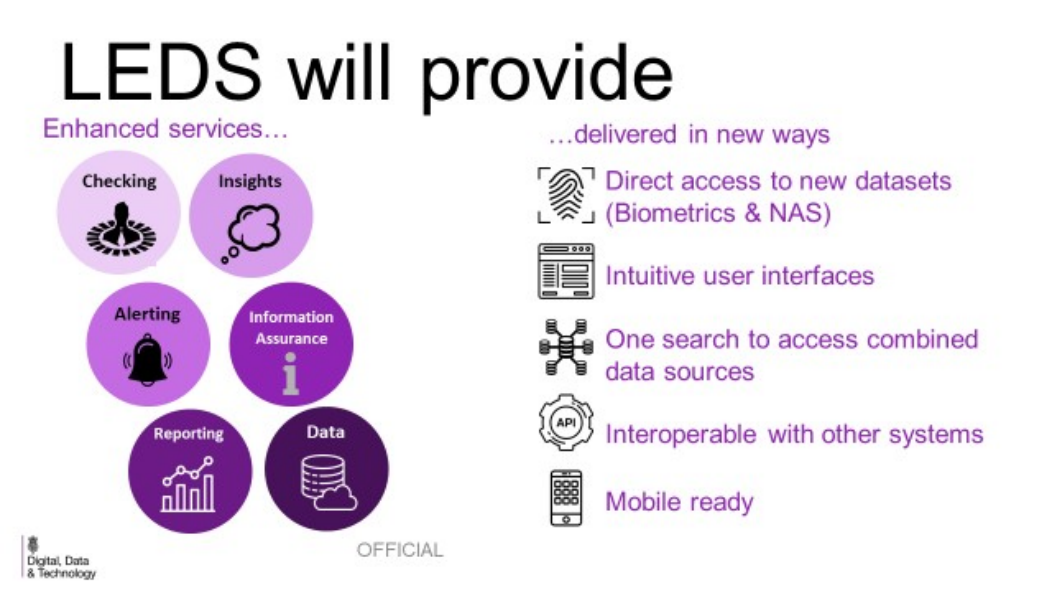
2 Background to LEDS and the Code of Practice

The National Law Enforcement Data Programme (NLEDP) was established to protect the public by building a modern and affordable Law Enforcement Data Service (LEDS) to replace the critical national public services currently provided by the Police National Computer (PNC) and the Police National Database (PND). LEDS will provide law enforcement and other agencies, on-demand and at the point of need, with current and joined up information in order to prevent crime and better safeguard the public. Historical and recent Serious Case Reviews (such as that following the Soham murders) has identified data sharing failures as a cause and crime is increasingly crossing regional and national borders.

Both the PNC and PND are reaching end of life. New technology and data sources cannot be used to enhance the PNC and PND, due to the limitations of these systems and there is a growing backlog of business demands for improvement. PNC and PND in themselves have therefore become a limiting factor in delivering improved data services for law enforcement.

The current PNC was initially designed over 45 years ago and is neither modern nor user friendly. LEDs will provide a more intuitive interface and users will receive full training and guidance to maximise the benefits of the enhanced capabilities. LEDS will be an end-to-end service bringing together nationally held information from PNC (and in due course PND) with the first National Missing Persons Register as an enhancement. Users will have limited access depending on their organisation, role within that organisation and a justified need to see specific data sets. LEDS will not replace all local policing data systems. Some data will therefore exist in two places simultaneously, on the originating data system (such as DVLA database) and a copy of certain data sets will go to LEDS. Some data will also be entered directly onto LEDS.

There are two existing separate codes of practice in existence for PNC and PND, with complex governance structures overseeing both systems. The former is used by Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) when it inspects police forces and other organisations. The College of Policing, which is the professional body for Policing in England and Wales was asked to produce a specific Code of Practice for LEDS, ready for first (beta) implementation when data from the newly created National Register for Missing Persons becomes available through LEDS.



THE PURPOSE OF THE CODE OF PRACTICE

7.1

The purpose of the Code is to support the ethical, fair, diligent and impartial use of the LEDS system. The Code supports key principles in upholding fundamental human rights, demonstrating equal respect to all people, and accordance with the law. The Code will achieve this through 5 equally important aims:

a) **Safeguarding people**: - Facilitating the use of data by law enforcement and other agencies at the appropriate time and in the appropriate way. Using accurate and joined-up information in order to bring offenders to justice, to prevent crime and better protect the vulnerable. Policing is however not always about crime and LEDS will also include the National Missing Person's Register to enable police to help locate those who are missing and safeguard those who may be vulnerable.

b) **Promoting accountability**: - Ensuring activities undertaken in relation to LEDS have clear lines of responsibility so that each organisation (users and suppliers of data) understands and can demonstrate that they comply with the principles underlying the Code.

c) **Promoting Understanding**: - Enabling greater understanding of the objectives of LEDS as a law enforcement information system. The Code uses plain language to enable the users of LEDS to be confident in the activities they need to undertake to prevent and detect crime, protect the public and safeguard the vulnerable. The public reader should be confident of the protections that the Code puts in place to preserve their data and privacy interests.

d) **Enabling Performance**: - Supporting performance through a quality management regime, which delivers continuous improvements to the value of the information within LEDS including; promoting better data quality, ensuring the relevance of the information and strengthening the partnership working where information is shared across organisational boundaries. This will be facilitated by training to support implementation and a requirement for organisations to pro-actively support continuous practice development and improvement amongst all users.

e) **Promoting Fairness**: - The public also need confidence in the relevance of the information held. The Code also supports the mechanisms (training, learning, development, audit and inspection) that will ensure that LEDS is not used in a way that is discriminatory or otherwise unfair to anyone based on their age, race,

ethnicity, any faith or belief, gender, gender identity, sexual orientation or disability. The Code will be regularly reviewed so it is consistent with evolving Human Rights, Data Protection and Ethical Standards. The Code will adhere to relevant data protection legislation and other principles, to advocate that information retained by law enforcement is constrained by what is considered fair, legal, proportionate and necessary.

3 WHO IS SUBJECT TO THE CODE?

3.1

As a code of practice, the legal status of the Code of Practice for LEDS applies to police forces in England and Wales. The College of Policing has a remit to issue a Code of Practice for LEDS under section 39A of the Police Act 1996 (as amended by section 124 of the Anti-Social Behaviour, Crime and Policing Act 2014).

3.2

The scope of the Code of Practice for LEDS is much wider, reflecting LEDS' use by other police forces outside of England and Wales), other law enforcement agencies and some non-law enforcement bodies with a limited law enforcement role. All user organisations will have to sign a data sharing agreement to access the Data in LEDS. This data sharing agreement will require compliance with the Code. That means the Code extends to all agencies, police forces, or other bodies that will be granted use of LEDS for policing or safeguarding purposes. LEDS may also be accessed by some commercial organisations under the data sharing agreements but access is limited to applications which support law enforcement purposes, such as checking for or preventing vehicle fraud. The Code will apply to these organisations as well.

4 WHO ARE THE ORGANISATIONS USING LEDS?

4.1

The Data Protection Act (DPA) 2018 defines the competent authorities processing data for law enforcement purposes as, but not limited, to:

a) the police, criminal courts, prisons, non-policing law enforcement agencies; and

b) any other body that has statutory functions to exercise public authority or public powers for any law enforcement purposes.

LEDS will initially be used by organisations that currently use PNC and PND. Requests for access to LEDS will be decided upon by a LEDS approval body, which will have membership from the National Police Chiefs 'Council (NPCC) the Association of Police Authorities and the Home Office.

Some of the agencies that currently use the Police National Computer (PNC) will transition over to use LEDS. These include bodies such as; Charity Commission for England & Wales, Department for Work & Pensions, Disclosure and Barring Service, Driver and Vehicle Licensing Agency, National Crime Agency, HM Prison and Probation Service, Royal Mail Security and Trading Standards.

The PND was set up following the Bichard Inquiry into the murders of Holly Wells and Jessica Chapman in Soham, where failures in police intelligence gathering and sharing were identified. In addition to the police a few other agencies access the PND. All access to PND information is solely for a "policing purpose". The prioritised uses of PND are the protection of children and young people, understanding and reducing the threat posed by terrorism and disrupting and preventing major, serious and organised crime. Access to these data sets will remain limited.

4.2

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. A full list of the current organisations which are signing up to the use of LEDS will be maintained by the Home Office and will be available online at xxxxxxxxxxxxxxxxxxx

5 WHO IS RESPONSIBLE FOR LEDS?

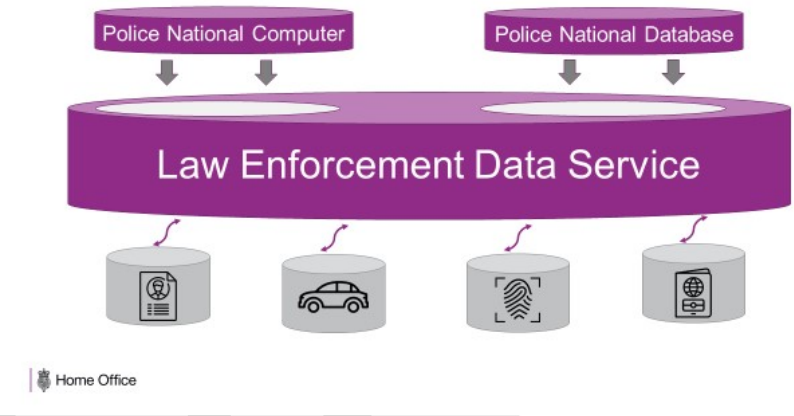
5.1

The Home Office run National Law Enforcement Data Programme (NLEDP) is responsible for all the design, development and governance of the emerging system, but will eventually be superseded by a LEDS governance body. The Home Office is the platform owner i.e. running the platform and shares some of the current governance responsibilities with the National Police Chiefs' Council (NPCC) as the co-ordinating body for those police forces which will input most of the data into LEDS. The NPCC provides leadership and direction to the police forces who will use LEDS.

5.2

Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) will have a role in inspecting how LEDS is being governed, managed and used and will issue guidance and recommendations. Scotland and Northern Ireland are not covered by section 1 of the Police Act 1996, and not subject to the same power of oversight by HMICFRS as they have their own legislation and governance, arrangements. HMICFRS is required to inspect the Police Service of Northern Ireland (PSNI) at least once in every year on its efficiency and effectiveness. Her Majesty's Inspectorate of Constabulary in Scotland operate separately. Engaging with HMICFRS for oversight of LEDS Code of Practice compliance will be included as a condition in the data sharing agreements, as it is with organisations who currently sign up to use the existing PNC and PND.

6 WHAT DETAILS MIGHT BE HELD ON LEDS?



Initially data from the PNC will be migrated into LEDS (by late 2021) before data from the PND (available 2023). The National Register of Missing Persons (NRMP) will start to exist on LEDS from 2020.

Personal information that might be held on LEDs includes biographical (such as name and Data of Birth) and contact information, but it can also include some biometric data (as well as other types of electronically held information such as body worn video or CCTV images.

LEDS will hold details of people who are, or were, of interest to UK law enforcement agencies because they:

- have convictions for criminal offences

- have been arrested
- have been charged
- have been detained under lawful powers
- are under suspicion
- are subject to the legal process, for example waiting to appear at court
- are wanted
- have certain court orders made against them
- have absconded (escaped) from specified institutions
- are disqualified from driving by a court
- have a driver record held at the Driver and Vehicle Licensing Agency (DVLA)
- hold a firearm certificate.
- have been victims of crime or witnesses to criminal acts.

Records of people who are missing or have been found will be held on the National Register of Missing Persons within LEDS. In the past details of missing people have only been kept on the PNC until they are located with information only being retained on force systems. The act of going missing is clearly not a criminal act but it would better safeguard vulnerable missing persons to be able to look back at past episodes of absence, or spot patterns. Data will be retained until six clear years have passed since the missing person was last found. The processing is necessary for reasons of substantial public interest, and to safeguard people from harm or to protect their well-being and to do so in the most efficient and effective way possible.

LEDS also holds details of UK registered vehicles, these details are copied from those held by the DVLA. These include vehicle details, registered keeper details, DVLA markers (alerts to special details), police reports, and vehicle insurance details. Sensitivity markers highlight e.g. public figures where some details can be blocked from general view.

LEDS will contain intelligence, information, for example records of allegations or where investigations concluded where no caution or conviction resulted. Intelligence information on LEDS could form part of a disclosure on an Enhanced DBS certificate under section 113(4) of the Police Act 1997. Disclosure of non-conviction/caution information on the PND is not automatic but is done on a case by-case basis following the exercise of police discretion. This will remain the case for LEDS.

As well as sharing data between registered users the data LEDS will process for law enforcement purposes will come from a wide variety of sources, including;

- international law enforcement agencies and bodies
- emergency services such as the Fire Brigade, National Health Service or Ambulance

- courts
- security companies who transfer prisoners
- partner agencies involved in crime and disorder strategies
- private sector organisations working with the police in anti-crime strategies
- voluntary sector organisations
- approved organisations and people working with the police
- persons arrested
- victims
- witnesses
- relatives, guardians or other persons associated with missing people
- individuals passing information
- local authority and private CCTV systems
- body worn video, operated by police officers
- custody images

7 RESPONSIBILITIES UNDER THE CODE

6.1

LEDS is being developed by the Home Office's National Law Enforcement Data Programme (NLEDP). The Code of Practice therefore applies to the Home Office with respect to its functions in developing, maintaining and securing the integrity of LEDS as an ongoing information service. It is also applicable to all organisations who are granted access to the system, through their chief officers, chief executive officers, managers, members and personnel who access the LEDS system as part of their responsibilities in a law enforcement role.

6.2

In order to highlight how these responsibilities operate at different levels the Code has been structured under sections which reflect data processing functions and then four different operating levels which describe appropriate responsibilities or obligations that describe the good practice for data processing for LEDS under those functions. There are also responsibilities for supporting functions in managing LEDS as a data service. Maintaining integrity and quality assurance of the service are 'golden threads' which run through the sections of the Code.

6.3

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

The Home Office: The programme of development for LEDS is currently managed by NLEDP which sits within the Home Office. For the purposes of the Code the Home Office is said to carry the governance responsibilities until that happens.

The organisation: This is the organisation which has been granted access to LEDS through a data sharing agreement. This responsibility is directed to the chief officer, or 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)

Operational managers: 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)

A LEDS user: This is an individual who has been vetted and granted access to access the functionality of the service. 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.

8 Law Enforcement Principles

8.1

The Code recognises the existing legal framework for the use of information in legislation relating to data protection and human rights, and references relevant legislation, such as the Human Rights Act 1998 (HRA), Data Protection Act 2018 (DPA), and the General Data Protection Regulation. In particular the application of Law Enforcement Principles set out under the DPA, Part 3.

Need a paragraph on HRA

8.2

The vast majority of the data in LEDS will come under Part 3 of the Data Protection Act (DPA) 2018. The remainder will come under the General Data Protection Regulation (where necessary as applied by the Data Protection Act) In comparison to the GDPR, Part 3 of the Act allows additional restrictions to be placed on the disclosure of data (for example to

prevent live operations being disrupted). As the data being held may well be more sensitive Part 3 places a higher requirement of level of data for non-law enforcement data, and like the GDPR, requires data to be rectified or erased if wrong, though restrictions can be placed on the rectification or erasure.

8.3

The Code of Practice supports the powers of the ICO, in relation to law enforcement processing. Part 3 of the DPA sets out specific advice for law enforcement authorities. The principles are broadly the same as those in the GDPR, but here are no principles relating to individuals' rights or overseas transfers of personal data, these are addressed in the Act separately. Transparency requirements are not as strict for law enforcement purposes, due to the potential to prejudice an ongoing investigation in certain circumstances. However, a Data Protection Impact Assessment for LEDS will make clear that information should be proactively published where this is possible to aid with accountability and governance.

8.4

Law enforcement organisations must be able to demonstrate overall compliance with all of the law enforcement data principles in Part 3 of the DPA:

- 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).

-

9 WHAT DO WE MEAN BY POLICING AND LAW ENFORCEMENT PURPOSES?

9.1

Policing purposes are defined 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.

9.2

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."

The Code of Practice addresses both Policing and wider law enforcement bodies and uses the term law enforcement purposes to encompass the purposes of both sets of bodies.

10 WHO ENFORCES BREACHES OF THE CODE?

8.1

The Code of Practice is statutory guidance which will be admissible in a court of law and in disciplinary proceedings. The Code makes reference to specific legal requirements and any breaches of these will 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.

Police forces have internal professional standards departments (PSDs) who play an important role in the maintenance of public trust and confidence. Professional standards actively examine the following; Counter Corruption, vetting, complaints and misconduct and governance. They carry out the process of vetting new police officers and police staff and contractors, manage misconduct and complaints and investigate any suspected corruption activities. It is a principle of policing that such issues are dealt with openly and robustly in accordance with the Policing Code of Ethics.

Police forces also have specific Audit departments for PNC and PND who will also have a responsibility to carry out this function for LEDS. Designated auditors have higher access levels and monitor for any use of the system which causes a concern. They pick random transactions (about 5% of transactions in any week) and then check back with the user. The system allows for ‘keystroke’ monitoring, as users have to confirm their identity it is possible to trace back each use of the system. Auditors check every registered use at least once per year as well as looking for unusual patterns of use such as access outside of shift hours, access to specific data which may need explanation. The system also has ‘reason codes’ so a user has to be able to demonstrate that use was indeed for a policing purpose and justify that it was proportionate to that purpose. If auditors have any concerns they can report these to Professional standards for a more detailed investigation.

That means that for example someone who accesses the data out of curiosity, because it might refer to a celebrity or checks on a vehicle for a friend who wants to buy it, are examples where the user will be in breach and will be subject to disciplinary proceedings. LEDS users who access computer systems for a non-authorised purpose are liable to be prosecuted for the criminal offences of 'unauthorised access' under section 1 Computer Misuse Act 1990 or obtaining or disclosing or procuring the disclosure of personal data for an unlawful purpose under section 170 Data Protection Act 2018

11 Can I access my data on LEDS?

LEDS is not open for public access. However there are a number of ways that members of the public can make enquiries about whether their data is held on LEDS and how it is used.

Checking convictions records.

The Disclosure and Barring Service helps employers make safer recruitment decisions each year by processing and issuing DBS checks for England, Wales, the Channel Islands and the Isle of Man. DBS also maintains the adults' and children's Barred Lists and makes considered decisions as to whether an individual should be included on one or both of these

lists and barred from engaging in regulated activity. A basic DBS check is for any purpose, including employment. The certificate will contain details of convictions and conditional cautions that are considered to be unspent under the terms of the Rehabilitation of Offenders Act (ROA) 1974. An individual can apply for a basic check directly to the DBS through their online application route.

In Northern Ireland Access NI on the official government website for Northern Ireland citizens www.nidirect.gov.uk perform the service of record checking for criminal record checks for people living or working in Northern Ireland. An individual can apply online for a basic check. You need an nidirect account to apply online. Disclosure Scotland provides the same service in Scotland

Subject Access Request

The Information Commissioner's Office (ICO) provides guidance on how to make a request for information. The right of access allows you to obtain personal information held about you by organisations, including police forces and the wider criminal justice system.

Data protection legislation protects personal data. It gives individuals the legal right to access information held about them by making a Subject Access Request. Data Subject Access Requests must be made 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. If you are unsure what information may be held on your record or if there is a record held in respect of you on the PNC or LEDS then you can apply for an ACRO Subject Access request.

Freedom of Information Act 2000

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. The FOIA places statutory obligations on public authorities to comply but is not a route to obtain personal data.

Individuals may want to seek to have their data on LEDS rectified for an inaccuracy, for example, there may be inaccuracies in the details of a criminal conviction held on LEDS. An individual may receive a copy of their criminal record and request that an incorrect entry for Grievous Bodily Harm is corrected to Actual Bodily Harm, or vice versa, to reflect the correct conviction. Individuals who believe that their data may be contained within LEDS without just cause, have the right to request the deletion or removal of their personal data and have a right to 'block' or restrict processing of their personal data. This will be done by direct

application to the force or agency that input the wrong data. The Information Commissioner's Office (ICO) provides guidance on how to make a request to have data rectified or removed The ACRO website contains a table individual force websites to enable that application to be made in writing.

Concerned parties who believe that there may be evidence of breach of the Code of Practice should in the first instance report those concerns to the Home Office, as the governance body for LEDS. The mechanism for reporting concerns is XXXXXX

12 Other Concerned Bodies

The Information Commissioner's Office, the UK's independent body set up to uphold information rights, has shown an interest in the development of LEDS and will be invited to formally respond to consultation. Other audit and oversight bodies, such as the Independent Office for Police Conduct, Policing Independent Review Commission, the Biometrics Commissioner and the Investigatory Powers Commissioner's Office will have an interest where the use of LEDS touches upon their responsibilities.

Need to put in contact details so hyperlink the names above and references below?

13 Relationship to other guidance

1. As discussed earlier, the UK data protection regime is set out in the Data Protection Act (DPA), 2018, along with the General Data Protection Regulation (which form part of UK law). The Information Commissioner's Office Guide to Law Enforcement Processing is a key driver in the Code of Practice.
2. Protection of Freedoms Act 2012 (POFA). This set out provision for deleting biometric data (DNA and fingerprint) in compliance with the circumstances and time frames set in place under the Act. The Act removed existing police powers to retain biometric data from suspects who are not or convicted of any offence. It also reduces the length of time for which data can be retained, with only the data of those convicted of the most serious offences being subject to 'indefinite' retention. The Home Office (2017) Review of the Use and Retention of Custody Images set out further out guidance about the retention of custody images which may have been kept on unconvicted individuals.

3. Investigatory Powers Act 2016 and the Data Retention and Acquisition Regulations 2018, provide guidance on retention and disclosure of communications and communications data acquired under the provisions of the Act.

4. The College of Policing produces Authorised Professional Practice (APP) which provides further detail to support expectations of good practice in policing. 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. Most APP is available open source. The Management of Police Information Code of Practice 2005 APP on Management of Police Information has reference to data retention in the section on Retention, review and disposal.

5. NLEDP or its successor will scan for changes to underpinning guidance, changes to legislation and make recommendations for further guidance