



Leicestershire Police

Information Management Policy

Policy Owner:	Head of Corporate Services
Department Responsible:	Information Management
Chief Officer Approval:	Deputy Chief Constable
Date of Next Review:	November 2025

This policy has been reviewed against APP and all relevant procedures.

Moved to APP:	Partly Moved to APP
Rationale:	Local policy requirements

This document has been produced in conjunction with the Leicestershire Police Legislative Compliance Pack

Review log

Date	Minor / Major / No change	Section	Author
25/06/2014	Minor	Change of organisational name and MoPI guidance changed to APP	Paul Hooseman, Impact Programme Manager and (Interim) Information Manager
15/08/2017	Minor	Change of Dept. Responsible, inclusion of GIRR and GSC	Paul Hooseman Information Manager
19/10/2018	Minor	GDPR / DPA 2018 Update	8870 Simon Adams IM Project Manager
11 Feb 2020	No change	N/a	7289 Ian Ginns
23 April 2020	Minor	Links to RM and Internet and Social Media policies updated	7285 Amanda McKenzie
16 Aug 22	Minor	EU GDPR to UK GDPR	7289 Ian Ginns
15 th Nov 23	Minor	Records Management	7022 Steven Morris
24/10/2024	None		7022 Steven Morris

1. Statement

Leicestershire Police has a duty to obtain and use a wide variety of information (including personal information) in order to discharge its responsibilities effectively. In compliance with the requirements of the statutory Code of Practice for the Management of Police Information, and associated Authorised Professional Practice for Information Management, the Force has adopted an Information Management Strategy. This Information Management Policy with its associated procedures supplements that strategy.

2. Aims

This Information Management Policy with its associated procedures provides a mandate for the performance of all information management functions within the Force and will assist the Force to comply with the relevant legislation and national guidance.

3. Scope

This policy applies to all information held and used by the Force including that used for policing duties and for administrative purposes such as HR, Finance, fleet, etc:-

The Code of Practice for the Management of Police Information defines policing duties/purposes as:-

- Protecting life and property
- Preserving order
- Preventing the commission of offences
- Bringing offenders to justice
- Any duty or responsibility of the police arising from common or statute law.

The Data Protection Act 2018 (DPA 2018) refers to the 'Law Enforcement Purposes. It defines these in Part 3, section 31 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."

UK General Data Protection Regulations (GDPR) extends the scope of this policy to include all other organisational information which does not fall under the MoPI COP.

This policy applies to all Leicestershire police officers, staff and volunteers who use organisational information as necessary to carry out their duties and to contractors, partner agencies or other individuals who may have access to or process police information on our behalf so as to ensure its use complies with relevant legislation and local policies and procedures.

Use of Information including Email and Internet

All information held by Leicestershire Police is for the purposes of policing across Leicestershire and Rutland and in the wider police community. The information is for use by all categories of individual mentioned above as is necessary to carry out their current role.

Individuals are not permitted to use police information for:-

- Their own personal use

- Out of casual curiosity
- For another person's curiosity
- Other than as permitted to perform their current role.

If there is any doubt the question "Am I doing this for policing or associated purposes?" should be considered. If the answer is 'No' then the activity should not be undertaken.

Individuals may be called upon to justify their actions not only as a result of routine auditing and monitoring but also following a complaint or discipline enquiry.

Use of email (internal and external) and the internet is only permitted in connection with policing or associated purposes. However, the Chief Constable has permitted use of external internet according to the [Internet Access and Social Networking Procedure](#). Leicestershire Police will provide feedback to staff who do not use or handle information in accordance with this policy/legislation and where necessary will initiate appropriate disciplinary action or a criminal investigation. Accessing or using information which an individual is not entitled to may be a criminal offence under the Computer Misuse Act 1990, the DPA 2018 or the GDPR.

Information Management covers a number of discrete but interrelated areas of business and the following section is a brief policy statement for each of these areas.

Data Protection Act 2018 & UK GDPR

Leicestershire Police is committed to ensuring officers, staff, and volunteers undertake their legitimate duties in a manner that is compatible with both the DPA 2018 and the GDPR and will endeavour to ensure that the data protection principles are applied to all personal information held and used by the Force.

The Force recognises the sensitivity of the personal information held and its duties in respect of such data to protect individuals from:-

- the use of incorrect information,
- the misuse of correct information,
- the unauthorised loss or disclosure of their information,
- the re-identification of de-identified personal data.

The Force recognises the individual's rights regarding access to, rectification of, erasure of or restricting the processing of personal information held by the organisation. It also recognises the individual's right not to be subject to automated decision making. This recognition is subject to the exemptions and restrictions outlined in both the DPA 2018 and the GDPR.

All subject access or subject rights requests are processed by the Force Information Management Section.

Public Interest / Substantial Public Interest

The term public interest has long been debated among scholars, politicians and philosophers alike. The general agreement on the term is that of what it is not rather than what it is: That is to say that most believe that public interest is NOT simply the wants or desires of a group of citizens or indeed the 'will or wants of interested factions'.

There are a number of factors such as the peace and safety of the public, their wellbeing as well as combining and translating many other factors into what might be deemed as the 'public good' which need to be considered whilst ensuring protections for minority groups. Additionally consideration would need to be given

as to the breadth and depth of the interest i.e is it local, regional or national and is it community based?

There is no one definition for Public Interest and each case has to be considered on its merits and impact.

The DPA 2018 Schedule 1, Part 2 references a number of circumstances where 'substantial' public interest conditions may be met.

These are:

- Statutory etc. and government purposes.
- Administration of Justice and parliamentary purposes.
- Equality of opportunity or treatment.
- Racial and ethnic diversity at senior levels of organisations.
- Preventing or detecting unlawful acts.
- Protecting the public against dishonesty.
- Regulatory requirements relating to unlawful acts and dishonesty etc.
- Journalism etc. in connection with unlawful acts and dishonesty etc.
- Preventing Fraud.
- Suspicion of terrorist financing or money laundering.
- Support for individuals with a particular disability or medical condition.
- Counselling etc.
- Safeguarding of Children and of individuals at risk.
- Safeguarding or economic wellbeing of certain individuals.
- Insurance.
- Occupational pensions.
- Political Parties.
- Elected representatives responding to requests.
- Disclosure to elected representatives.
- Informing elected representatives about prisoners.
- Publication of legal judgements.
- Anti-doping in sport.
- Standards of behaviour in sport.

Although comprehensive this does not capture everything which could be deemed as significant, nor does it capture the lower public interest considerations. As such; Leicestershire Police recognises its diverse communities and accepts that it needs to consider what is within the parameters of 'Public Interest' on a case by case basis.

Where this is considered and it falls outside the list given above, it will be recorded and a summary of the circumstances captured in a public interest appendices to this policy.

Data Quality

The principles of the DPA 2018 and the GDPR require the Force to ensure that personal information is accurate, relevant and up to date. In addition, data quality is integral to effective policing by ensuring that accurate exploitable and up-date information is available, when it is needed.

Failing to achieve an appropriate level of quality for Force information can present operational problems, for example failing to identify a vital link between records, making a false arrest, executing a warrant at the wrong address or making an inappropriate or misleading disclosure. It can also have legal implications in terms of failure to comply with the DPA 2018, the GDPR, the Human Rights Act 1998 and

the Freedom of Information Act 2000 (FOIA). It may also leave the Force vulnerable to civil litigation or enforcement action by the Information Commissioners Office (ICO) over the use of incorrect information.

The Force will continue to apply the range of activities identified in the [Data Quality Strategy](#) in order to improve data quality throughout Force business areas.

Records Management

Leicestershire Police is committed to improving records management to support the Force by ensuring information is managed throughout its life cycle in a systematic, cost- effective and efficient manner. In particular, it provides a means of applying controls to information to maintain its evidential weight and ensure its authenticity, availability and integrity.

Good practice in records management ensures that information in any format is readily available for policing use which includes sharing with partner agencies where necessary. As such, it will underpin compliance with the MoPI Code of Practice, the DPA 1998, GDPR, FOIA and other relevant legislation.

Compliance with [records management policy](#) and standards contributes towards the avoidance of significant risk to the Force by enabling and providing evidence of transactions, thereby reducing vulnerability to legal challenge.

Records Management, through the proper control, review, retention and disposal ensures compliance with our legal obligations, reduces organisational cost, and promotes best value in terms of storage resource.

Statutory Code of Practice on the Management of Police Information and associated Authorised Professional Practice

This Code of Practice and associated guidance provides national standards for police information management to support the establishment of a common infrastructure for policing and meets the recommendations of the Bichard Inquiry.

It provides guidance on the collection, recording and evaluation of policing information as well as effective intelligence management. A key feature is the linking of information / intelligence about people, objects, locations and events held in various systems both in Force and held by other Forces to build a composite picture and enable appropriate action to be taken and risk based decisions to be made about priorities.

Leicestershire Police recognises that the collection of appropriate information with a high standard of data quality, its accurate assessment and timely exploitation are core to efficient policing and is committed to implementing this legislation and guidance with particular emphasis on maximising the benefits which this will bring to operational policing.

Information Assurance

The Force is committed to compliance with the sixth data protection principle which requires an organisation to apply appropriate technical or organisational measures in order to protect the personal information which it holds. It also recognises the distress, damage and harm which may be caused to individuals should information about them be lost or disclosed inappropriately.

The Force seeks to apply the [HMG Management of Risk in Government](#) framework and guidance to its information management practices and the Force Information Security Policy supports this.

The Force has adopted the [Government Security Classifications](#) (GSC) and the associated handling rules and encourages partner agencies to apply the Force security standards to police information through the use of Information Sharing Agreements.

Freedom of Information Act 2000

Leicestershire Police is committed to adopting an open and transparent approach in relation to the policing of Leicestershire. It is cognizant of its statutory duties and endeavour to proactively publish information as far as is possible without compromising its policing purposes in compliance with the Freedom of Information Act and Article 86 GDPR.

Requests for information made under the Freedom of Information Act 2000 will be processed by the Information Management Section in accordance with the [Freedom of Information Procedural guide](#). Consultation will take place as necessary with the Business Owner who holds the information which has been requested and exemptions will be applied in accordance with the legislation when disclosure of the information would cause harm, eg, to an individual, to effective policing, etc.

Information Sharing

Leicestershire Police is a signatory to the Leicestershire [Information Sharing Protocol \(ISP\)](#). A number of public, private and voluntary organisations within the County have signed the ISP and committed to the principles of information sharing where this is necessary to enable them to carry out, or to support their partners to achieve, their statutory responsibilities.

Personal information received by the Force may be shared with other agencies where this is necessary for the law enforcement or policing purposes outlined above or where there is a lawful basis for the personal information to be shared with another agency to enable that agency to carry out their statutory responsibilities.

The Force will also share non personal information for those same purposes.

Leicestershire Police recognises a specific duty to work with and share information with partner agencies in high risk areas such as children and vulnerable adults. This is supported at strategic level by the Office for the Police and Crime Commissioner, the local strategic partnerships and the Crime and Disorder Reduction Partnership (CDRP) structures which are in place.

When it is necessary to share information urgently to safeguard children and vulnerable adults, this will usually be through the Child Abuse Investigation Unit (CAIU), however, Chief Officers will support any information sharing carried out under urgent circumstances for these purposes. The information shared in these circumstances must be documented.

When the intention is to share information on a regular basis the Force supports the production of Information Sharing Agreements. An Information Sharing Agreement (ISA) is a formal written arrangement between organisations when it is necessary to share personal (or occasionally non personal) information on an ongoing basis. An ISA can enhance effective multi-agency working for the Force but also provides protection by documenting the process.

- Ensuring that information can be shared lawfully
- Ensuring consistency in the way information is shared
- Allowing the Force to specify conditions on the way information can be used by the partner agency

- Allowing the Force to agree the appropriate security measures to be applied to the information.

This enables the Force to share information in compliance with the DPA 2018 and GDPR.

Disclosure

Leicestershire Police is committed to building a safer community by working with local partners. The Force strives to achieve a sustained multi-agency approach to policing and encourages the exchange of information within the law, in order to reduce crime and the fear of crime and disorder in our community.

The DPA 2018 and the GDPR provide guidance in relation to the use and processing of personal information including the disclosure of such information.

The ability and the requirement to disclose non-personal information has been extended across the public sector by the Freedom of Information Act 2000, which places specific obligations on all public sector bodies to make more information available to the public about any aspects of their functions.

A number of policies and procedures exist to guide the various disclosure processes. This policy outlines general guidance on the principles of disclosure that can be applied where an existing process does not exist.

Where an ad hoc request for information is made this should identify a legal gateway – in most cases this means that the request for the information will be made under a statute. Where no legal gateway exists, the requestor should identify a statutory obligation which cannot be achieved without the disclosure of the information. In these cases, the Force will disclose the information if this does not impact upon any current policing process or the inherent rights of the data subject.

If an officer identifies a risk to individuals during an investigation and believes it is necessary to proactively disclose information over and above routine disclosures made as part of a police investigation, and this disclosure will have a significant impact upon the person under investigation (such as to the employer) this risk assessment process should be used and authorisation gained from an officer of NPCC rank – unless the delay caused by such a process would cause harm or a further crime to be committed.

Where an officer identifies a 'Vital' interest of an individual or another they may disclose personal information in pursuit of the protection of that Vital interest under Article 6(1)(d) of the GDPR and/or Section 30, 70 and schedule 8(3) of the DPA 2018. In these circumstances a 'Vital' interest would relate to the life or death of an individual. All such disclosures must be recorded and subsequently reviewed by an NPCC rank within the Force.

The Information Management Section

The Information Management Section sits within the Corporate Services Directorate of Leicestershire Police. The Section is responsible for Information and records management across the organisation and responding to requests for information including those received under the GDPR, DPA 2018 or the FOIA 2000.

4. Legal Basis

Legal basis is derived from the Police Act 1996 which gives a Constable certain powers. Section 30(1) gives constables all the powers and privileges of a constable throughout England and Wales and Section 30(5) defines these powers as powers

under any enactment whenever passed or made. These powers include the investigation and detection of crime, apprehension and prosecution of offenders, protection of life and property and maintenance of law and order.

In accordance with the DPA 2018 & GDPR the Data Protection principles must be adhered to in accordance with the purpose and/or use of the information.

The Human Rights Act 1998 requires public authorities, including police forces, to act in a way that is compatible with the European Convention on Human Rights. In relation to record retention this requires a proportionate approach to the personal information held about individuals.

The principles of the Code of Practice (2005) relating to the Management of Police Information will be given due regard by Chief Officers of Police.

5. Audit & Monitoring

Leicestershire Police is required to ensure data held in hard copy or police computer systems is obtained, held, used and disclosed in accordance with the GDPR and/or the DPA 2018, the statutory Code of Practice for the Management of Police Information 2005, the associated Authorised Professional Practice (APP) for Information Management and relevant NPCC policy and procedures.

Business owners have responsibility for ongoing monitoring of information obtained, held, used and disclosed in their area of business as well as for the data quality. The DPA 2018 has six principles which include the following:-

Data should be:-

- Adequate, relevant and not excessive in relation to its registered purposes(s)
- Accurate and where necessary kept up to date; and
- Kept for no longer than is necessary for its registered purpose.

The Force Audit Strategy determines the nature and scope of the audits and provides a three-year audit plan taking into account the resources available, the changing environment and national requirements.

Major influencers on the police service and subsequently upon the audit function are the MoPI COP, the APP for Information Management which gives further detail to Forces on the practical implementation of the Code, the GDPR which covers the use of organisational information which falls outside the scope of MoPI and the DPA 2018 which covers the application of the GDPR for Law Enforcement Purposes.

The underlying purpose of the APP, Code and legislation is to ensure forces have processes in place to identify all information held about individuals, be able to properly protect use and manage that information and to readily identify individuals who cause the most harm or risk to society.