

Lincolnshire Police

Policy Document



Data protection and freedom of information policy

PD 141

Policy document information

Reference number:	PD 141
Policy sponsor:	Chief Technical Information Officer (CTIO)
Policy owner:	Head of IMU – Jen Johnson
Reviewing officer:	Data Protection Supervisor – Jana Randle
Publication date:	November 2025
Review date:	November 2027

Version history

Version	Date	Reason for issue
16	July 2019	Minor amendments
17	November 2019	Biennial Review
18	November 2021	Biennial Review
19	November 2022	Minor amendments
20	November 2023	Biennial Review
21	November 2025	Biennial Review

Code of Ethics

All staff involved in carrying out functions under this policy and associated procedures and appendices will do so in accordance with the principles of the Code of Ethics. The aim of the Code of Ethics is to support each member of the policing profession to deliver the highest professional standards in their service to the public.

Legislative compliance

This document has been drafted to comply with the principles of the Human Rights Act. Proportionality has been identified as the key to Human Rights compliance, this means striking a fair balance between the rights of the staff and those of the rest of the community. There must be a reasonable relationship between the aim to be achieved and the means used.

Equality and Diversity issues have also been considered to ensure compliance with the Equality Act 2010 and meet our legal obligation in relation to the equality duty. In addition, Data Protection, Freedom of Information and Health and Safety Issues have been considered. Adherence to this policy or procedure will therefore ensure compliance with all relevant legislation and internal policies.

Other legislation/law which this policy has been drafted to comply with:

- [Human Rights Act 1998 \(in particular A.14 – Prohibition of discrimination\)](#)
- [Equality Act 2010](#)
- [Crime and Disorder Act 1998](#)
- [H&S legislation](#)
- [Data Protection Act 2018](#)
- [Data \(Use and Access\) Act 2025](#)
- [Freedom Of Information Act 2000](#)

Security classification

Policy to be published on Intranet: Yes

Policy to be published on Force Website: Yes

Authorised Professional Practice (APP)

This Policy has been checked against APP. Lincolnshire Police has adopted the APP provisions, with supplementary information contained herein, which reflects local practice and the needs of the communities served by Lincolnshire Police.

Those provisions are shown in the links below and can be accessed via the home page of the APP website:

<https://www.app.college.police.uk/app-content/information-management/data-protection>

1. Policy aims (Purpose)

- 1.1. The main aim of this policy is to ensure that Force-owned personal information is used appropriately in compliance with the requirements of the Act and that all officers and staff are clear about what is regarded as acceptable and what is improper use.
- 1.2. The policy is underpinned by procedure that sets out minimum standards and details how those employees and any other authorised person having

access to any force systems may use Force-owned personal information lawfully.

1.3. There are 6 Principles under GDPR and Data Protection Act 2018

- Principle 1 – Lawful, Fair and Transparent
- Principle 2 – Specified, explicit, legitimate
- Principle 3 – Adequate, relevant and Limited to what is Necessary.
- Principle 4 – Accurate, up to date
- Principle 5 – Kept no longer than necessary
- Principle 6 – Processed in a secure manner.

2. Policy statement (Key information)

2.1. The principles and scope of the policy

2.1.1. Lincolnshire Police is committed to ensuring that all its officers, staff and agents undertake their legitimate duties in a manner compatible with data protection principles set out in the UK General Data Protection Regulations (UK GDPR) (EU) 2016/679 and the Data Protection Act 2018 (herein after described throughout this policy as 'the Act').

2.1.2. The Act regulates the use of information from which a living individual can be identified. It applies to the processing of personal data in most formats including electronic, paper and other media.

2.1.3. A broad objective is to protect individuals from the use of inaccurate personal information, or misuse of accurate personal information. More specific associated objectives are to:

- a. Ensure all persons having access understand their responsibilities regarding their use of personal information.
- b. Eradicate unlawful use of personal information.
- c. Safeguard all personal information.
- d. Protect the reputation of Lincolnshire Police by strict compliance with the Act and MOPI guidance.

- 2.1.4. A right for an individual to access information held about them is provided by the UK General Data Protection Regulations (UK GDPR) (EU) 2016/679 and the Data Protection Act 2018, whilst the Freedom of Information Act 2000 provides a right to public access to information held by public authorities. This can be achieved by information published by Lincolnshire Police on the Publication Scheme or by a Member of the Public submitting a request to Lincolnshire Police.
- 2.1.5. All police officers, police and partnership staff, including the extended police family and those working voluntarily or under contract to Lincolnshire Police who have access to personal information must be aware of, and are required to comply with, all relevant policy and associated procedures.
- 2.1.6. This policy applies to persons at all levels of the organisation including all Police Officers, Police and Partnership Staff, Special Constabulary, PCSOs, temporary staff, partner agency staff, consultants, contractors and volunteers.
- 2.1.7. Lincolnshire Police will take criminal and/or disciplinary action against any category of person mentioned above who wilfully accesses and/or misuses personal information held by Lincolnshire Police.
- 2.1.8. Any use of personal information that does not have a clear policing or other statutory or business purpose is likely to constitute a misuse. Using information is described as “processing” in the Act. See Part 1 3(4) of the Act that describes the ways in which data is defined as having been processed (used).
- 2.1.9. Part 6 Section 170 of the Act identifies the following criminal offence:
- (1) It is an offence for a person knowingly or recklessly
- a. to obtain or disclose personal data without the consent of the controller
 - b. to procure the disclosure of personal data to another person without the consent of the controller, or

- c. after obtaining personal data, to retain it without the consent of the person who was the controller in relation to the personal data when it was obtained.

The Chief Officer lead for this policy is the Chief Digital Information Officer.

- 2.1.10. All police officers, police and partnership staff, including the extended police family and those working voluntarily or under contract to Lincolnshire Police who have access to personal information must be aware of, and are required to comply with, all relevant policy and associated procedures.

3. Other related documents and appendices

3.1. Appendices.

- Appendix A – Processes & Procedures
- Appendix B – Freedom of Information process
- Appendix C – Security Incident Reporting
- Appendix D – Serious Breach Impact Assessment
- Appendix E – Data Protection and SAR/Right of Access guidance
- Appendix F – General Processing Rectification process
- Appendix G – General Processing Restriction process
- Appendix H – General Processing Erasure & Objection process
- Appendix I – Law Enforcement Erasure or Restriction process
- Appendix J – Rectification process
- Appendix K - Subject Access Request/Right of Access Form
- Appendix L – Disclosing information to MPs

Related documents

- Force Security Policy (PD 55)
- GSC Policy (PD 228)
- GPMS Policy (PD 119)
- DPIA Policy (PD 170)
- Information Sharing Policy (PD 132)

- Review, Retention & Disposal (RRD) Policy (PD 54)
- Retention of Documents held for Non-Policing Purposes Policy (PD 156)
- Information Audit & Procedures Policy (PD135)
- PND Audit Policy (PD179)
- PNC Policy (PD128)
- ACPO (2011) Manual of Guidance on the FOI (2000)
- Information Management Strategy
- The Information Commissioner's Subject Access Code of Practice

4. Monitoring and review

- 4.1 Subject to any new legislation or changes in case law, which require immediate amendments, this document will be reviewed on a biennial basis by the Data Protection & FOI Manager in the IMU.

5. Who to contact about this policy

- 5.1. This policy is owned by the Head of IMU and any enquiries about this policy should be directed to Jen Johnson, Head of IMU, 07799 079921, jennifer.johnson@lincs.police.uk.