Lincolnshire Police

Policy Document

Force security policy PD 55

Policy document information

Reference number:	PD 55
Policy sponsor:	Chief Constable
Policy owner:	Deputy Chief Constable
Author:	Information Security Officer
Publication date:	May 2026
Review date:	May 2028

Version history

Version	Date	Reason for issue
22	May 2018	Early completion of the annual review due to GDPR implementation
23	Feb 2019	Minor amendment to App 1
24	Jul 2019	Amendment to App 1 - Access to Force information and systems
25	May 2020	Biennial Review
26	April 2022	Removal of G4S specific information and addition on Solo & Mitie Contractors.
27	May 2022	Biennial Review
28	Sep 2022	Addition of mandatory disk encryption when sending data to third parties.
29	April 2023	Amendment to removal of hard copy information from force premises.
30	Aug 2023	Amendment to Appendix 6
31	Sep 2023	Amendment to Appendix 1, password policy
32	May 2024	Biennial Review
33	June 2024	Update to Data Breach section of Appendix 1 and Appendix 7 SyOps
34	October 2024	Update to the Use of Personal Devices section of Appendix 1
35	December 2024	Inclusion of vulnerability management timescales within Appendix 1
36	May 2026	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
- Freedom Of Information Act 2000

Security classification

Policy to be published on Intranet: Yes

Policy to be published on Force Website: Yes (minus appendices)

Authorised Professional Practice (APP)

This policy has been checked against APP and there is none in relation to the subject matter of this policy.

1. Policy aims (Purpose)

1.1. The Force Information Security Policy applies to all manual and electronic information processes owned by Lincolnshire Police. The scope of this policy includes future adaptations in line with the NEP and the Office 365 suite, whether they are stored on premises or in the cloud.

The policy provides a common basis for the Force to develop, implement and measure effective information security management practice.

1.2. The policy applies to all Police Officers, Police Staff and all personnel contracted to work for Lincolnshire Police, Special Constables, Volunteers, temporary personnel and trusted employees from agencies and organisations who by the nature of their role require access to Lincolnshire Police information systems.

1.3. This policy is written in compliance with the Police Digital Services (PDS) Information Systems Community Security Policy, HMG's Security Policy Framework (SPF) and BS ISO/IEC 27001:2005: Information Security Management Systems – Requirements. These include the following:

- Security policies
- The security structure
- Asset classification and control
- Physical and environmental security
- Access control
- Systems development and maintenance
- Contractual controls
- Training and awareness
- Business continuity planning
- Compliance checking

1.4. The Force Information Security Policy has been produced to provide baseline security requirements in order to safeguard the confidentiality, integrity and availability of all information held by the Lincolnshire Police. The purpose of this policy is not to obstruct but enable the information sharing processes of the Lincolnshire Police. All personnel with access to information owned by the Lincolnshire Police will be made aware of and required to comply with the provisions of the policy.

1.5. The policy sets out to implement the requirements of the PDS Information Systems Community Security Policy together with the business and operational demands of the Lincolnshire Police.

2. Policy statement (Key information)

2.1. The origins/background information

2.1.1. Lincolnshire Police is dependent upon information, and consequently on the systems upon which information is processed. This policy sets out the strategic aims and objectives of the Force in relation to information protection for manual, electronic and mechanical systems.

2.1.2. Due to the current dependence of almost all organisations upon information communications technology (ICT), as might be expected, the content of this document includes many references to ICT information systems. However, the security of manually held information is equally important and, where appropriate, is covered in some detail in the relevant areas of the policy framework.

2.1.3. The general public has a right to expect that all members of the Force will, when utilising information in connection with Force business, ensure its confidentiality and integrity (particularly in relation to personal information) and availability. It is important that the right information is made available to those who need to use it for either operational or administrative purposes. When considering the availability of information employees should understand the benefits of making information available to those who ‘need to know' and therefore should follow relevant guidance when supplying information.

2.1.4. The loss, damage, wrongful destruction or wrongful disclosure of information could result in substantial costs to the Force as well as public embarrassment and a reduction in public confidence.

2.2. Motivators/Driving Forces

2.2.1. The Police Digital Services Community Security Policy (CSP) and Security Policy Framework (SPF) are intended to provide a common basis for the 'policing community' to develop, implement and measure effective security management practice and to provide confidence in inter-community dealings and third party access/supply.

2.3. General Principles of the Policy

2.3.1. The key area of this policy ensures that Lincolnshire Police, in common with the rest of the Police Service, acts appropriately in order to maintain the confidentiality, integrity and availability of the information that it holds. This applies to its own information or that which it has been entrusted by other organisations.

2.3.2. The procedures developed to support this policy will be at Appendix 1-4 and will contain appropriate guidance to staff. It is the responsibility of all staff to ensure that they are familiar with and adhere to these procedures.

2.3.2. It is the responsibility of each employee to adhere to this Policy and to:

- Comply with general security instructions,
- Comply with the force Generic Security Operating Procedures.
- Report any security incidents in accordance with agreed procedures.
- Advise line managers and the Information Security Officer, as appropriate, of any potential weaknesses in information security or associated procedures.

2.4. Legal Basis

2.4.1. The Force and its employees have an obligation to comply with United Kingdom and European Community legislation in respect of the use of information processing systems. This legislation includes:

- The Freedom of Information Act 2000
- The Data Protection Act 2018
- The Human Rights Act 1998
- The Copyright, Designs and Patents Act 1988
- The Computer Misuse Act 1990
- The Official Secrets Acts 1911,1920 and 1989

2.4.2. Human Rights Considerations/Articles Engaged

2.4.3. The implementation of the MoPI guidance and codes of practice or indeed the failure to do so correctly, could have implications for Lincolnshire Police under the following articles of the Human Rights Act:

- Article 2-Right to Life.
- Article 5-Right to Liberty and Security.
- Article 8-Right to respect for Private and family Life.

3. Other related documents and appendices

3.1. Appendices:

- Appendix 1 – Force Security Procedures
- Appendix 2 – Security Incident Response for Breaches of Personal Data
- Appendix 3 – Serious Brach Impact Assessment
- Appendix 4 - Force Internet and E-Mail Procedures
- Appendix 5 – Security Incident Report Form
- Appendix 6 – Generic SyOps

- Appendix 7 – Third Party Access Form

These appendices are protectively marked and therefore are only available on the Force internal Intranet. Any questions regarding the appendices should be directed to the Vetting & Security Manager.

- PDS Community Security Policy (CSP)
- Security Policy Framework (SPF)
- HMG Information Security Standards
- ISO/27001
- Management of Police Information (MoPI)
- Force Security Procedures
- Government Protective Marking Scheme (GPMS) Policy
- Government Security Classification (GSC)
- Force Vetting Policy
- Mobile Data Policy
- Audit Policy
- Business Continuity Policy
- Disaster Recovery Policy
- Change Control Policy
- Forensic Readiness Policy
- Remote Access Policy
- Hybrid Working Policy
- Protecting Data Stored On Portable Media Policy

4. Monitoring and review

4.1 This policy is a live document and as such will be under constant review dependent on the state of related national policy and the threat landscape.

The IMU information security officer is responsible for the review and update of this policy.

5. Who to contact about this policy

5.1. This policy is owned by Information Manager, Information Management Unit. Any enquires about this policy should be directed to the Vetting & Security Manager.