East Midlands Region

Policy Document

Regional Government Security Classification Scheme (GSC) policy PD 228

Policy document information

Reference number: PD 228

Policy sponsor: DCC Nottinghamshire Police

Policy owner: Regional Information Assurance Staff

Author: Layla Hughes, Vetting & Security Manager, Lincs Police

Publication date: September 2024

Review date: September 2026

Version history

Version	Date	Reason for issue
2	September 2017	Annual Review
3	May 2018	GDPR Review
4	September 2018	Biennial Review
5	April 2020	Addition of NEP Cloud
6	September 2020	Biennial review
7	September 2022	Biennial review
8	September 2024	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
- General Data Protection Regulations (EU) 2016/679 (GDPR)
- Freedom Of Information Act 2000

Security classification

Policy to be published on Intranet: Yes

Policy to be published on Force Website: Partially

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 purpose of this policy is to ensure that the East Midlands Forces comply with the requirements of the Government Security Classifications (GSC) and to provide instruction for the marking and handling of information.

1.2. This policy provides a framework for classifying information, and directs users to particular levels of control which are required to ensure the continuing Availability, Integrity and Confidentiality of information. The criteria for determining the correct classification must consider both the level of threat posed to the information and the impact it would have should the information be compromised.

1.3. This policy describes how The East Midlands Forces classify Information Assets to ensure they are appropriately protected and supports policing business processes by ensuring the value of information to the region is fully exploited. The policy applies to all the information that each Force collects, stores, processes, generates or shares to deliver services and conduct business of policing, including information received from or exchanged with other Police Forces and third-party suppliers.

2. Policy statement (Key information)

2.1. The policy detail should be placed here. Section headings might include:

- Principles and scope of the policy
- Motivators and driving forces
- Implications (of breaches, etc).

Avoid the use of unexplained acronyms, jargon and localisms and provide definitions and explanations for clarity where required.

2.1. General Principles

2.1.1. This policy sets out the East Midlands Forces' commitment to the management of police information. It also sets out what police personnel and delivery partners / third party suppliers should do to manage police information. In doing so, this policy supports the East Midlands Forces' strategic aims and objectives and should enable employees throughout the organisation and external support personnel to identify an acceptable level of risk and use appropriate handling controls.

2.1.2 All information that the East Midlands Forces need to collect, store, process, generate or share to deliver services and conduct police business has intrinsic value, and all staff must apply the appropriate degree of protection. 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.

2.1.3. All staff should apply this policy and ensure that consistent controls are implemented throughout the police service, delivery partners and wider supply chain. Delivery partners and suppliers who have access to the East Midlands Forces' information must apply equivalent controls, which should be provided for under contractual provisions or Information Sharing Agreements.

2.1.4. The East Midlands Forces Information Assets must be classified into three types: OFFICIAL (including the caveat of OFFICIAL – SENSITIVE), SECRET or TOP SECRET.

2.1.5. Everyone who works within the East Midlands Forces has a duty to respect the confidentiality and integrity of all information and data that they access, and is personally accountable for safeguarding information assets in line with this policy.

2.1.6. Staff must risk assess sharing information and only share information with those who have a legitimate need to see it.

2.1.7. Each classification requires a minimum set of security controls to be in place to provide the appropriate protection against a range of threats.

2.1.8. Access to any information must only be granted on the basis of a genuine need to know and an appropriate personnel security control (i.e. vetting level).

2.1.9. Disciplinary action will be considered for any member of staff (including contractors, consultants, and suppliers so far as is feasible) who do not follow the mandatory actions set out in this policy.

2.2. Applying the Government Security Classifications (GSC)

2.1.9. Disciplinary action will be considered for any member of staff (including contractors, consultants, and suppliers so far as is feasible) who do not follow the mandatory actions set out in this policy.

OFFICIAL

The majority of information that is created / processed by the East Midlands Forces.

Includes routine business and policing operations, including staff personal information, and non-policing services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile.

OFFICIAL – SENSITIVE should be used where there is a clear and justifiable requirement to reinforce the ‘need to know’ principal and carries a higher risk and could have severely damaging consequences if compromised.

SECRET

Very sensitive information that justifies heightened protective measures to defend against determined / highly capability threats.

The East Midlands Forces handle only a small amount of this type of information and you normally would not handle it.

Where compromise may seriously damage Critical National Infrastructure, international relations or the investigation of serious organised crime, or lead to loss of life.

Specialist areas such as Special Branch will handle information at this classification.

TOP SECRET

HMG’s most sensitive information requiring the highest levels of protection from the most serious threats.

Where compromise could cause widespread loss of life or else threaten the security or economic well-being of the country or friendly nations.

You are extremely unlikely to see this type of information in the East Midlands Forces

2.2.2. The Classifications do not have any direct implications for access to information under either the Data Protection Act (2018) or the Freedom of Information Act (2000). If information has a classification or marking, this does not mean that it is exempt from being disclosed, and if information does not have a marking, this does not mean that it can be automatically disclosed. The existence of a protective marking might help to make a decision about access, but every case must be considered on its own merits.

2.3. OFFICIAL classification

2.3.1. This classification applies to the vast majority of the East Midlands Forces' information including:

- General day to day policing activity
- Most front line service operations
- Organisation and performance management information
- Personal information (including staff data, case files, citizen data)
- Business information (finance, estates, personnel, policy, commercial)
- Policy documents

2.3.2. The OFFICIAL classification reflects the fact that reasonable measures need to be taken to look after an Information Asset and to comply with relevant legislation such as the Data Protection Act 2018.

2.3.3. The controls in place must be sufficient to protect against a range of impacts and threat actors such as hacktivists, single issue pressure groups, investigative journalists, competent individual hackers, and the majority of criminal individuals or groups.

2.3.4. **All information should, as a minimum, be treated as OFFICIAL.**

2.3.5. Any information which does not have a marking should be treated as OFFICIAL and handled accordingly.

2.3.6. A limited amount of OFFICIAL information could have more damaging consequences if lost, stolen or published in the media. This subset of information should still be managed within the OFFICIAL classification, but as it has a higher impact if compromised should attract additional control measures (generally procedural or personnel), to reinforce the 'need to know' principal. In these cases where there is a clear and justifiable requirement, then information can be described using the caveat of SENSITIVE i.e. **OFFICIAL - SENSITIVE**.

2.3.7. Examples of where the OFFICIAL – SENSITIVE classification should be used include:

- Where the outcome of a risk assessment highlights a specific risk, or threat to highly vulnerable individuals.
- Cases involving intimidation, corruption or fraud.
- Where there is a legal requirement for anonymity.
- Where there is a high media profile and risk of damaging reputation under unauthorised disclosure.
- Highly sensitive change proposals or contentious negotiations
- Highly sensitive operational procedures.
- Major security or contingency planning details.

2.3.8. **This more sensitive information must be identified by being marked OFFICIAL - SENSITIVE. This marking alerts users to the enhanced level of risk and that additional controls are required, such as handling instructions.**

2.3.9. For more information on applying classifications and handling information, refer to Appendix 2, Information Asset Control Measures.

2.4. SECRET Classification

2.4.1 The SECRET classification must only be used where there is a high impact of risk and a sophisticated / determined threat from such elements as serious and organised crime and foreign intelligence services.

2.4.2. Examples of SECRET include:

- Classified material received from Government Departments / agencies relating to National Security and Counter-Terrorism.
- Intelligence and investigations relating to individuals of interest to security agencies.
- Information that could cause serious damage national security and intelligence operations.
- Information affecting the ability to investigate or prosecute serious/organised crime where there is intelligence to suggest there is a known sophisticated and determined threat to access the information.
- Personal/case details where there is a specific threat to the life/liberty of an individual such as protected witness scheme records.

2.4.3. The concept of sophisticated or heightened threat does not only apply to those with a high technical (e.g. IT) attack capability. It can apply to criminals who have a developed capability to intimidate or coerce individuals i.e. if disclosure of information could result in serious physical harm or put a life at risk because there is a real and highly capable threat present, the information must be tightly controlled.

2.4.4. **SECRET** must not become the default status for material just because of the type of case or potentially severe consequences (e.g. murder trials, or where there is a threat to life). The threat capability must also be present. There is no change to controls at this level.

2.4.5. The East Midlands Forces will only handle a very small amount of information at this classification in areas such as Special Branch.

2.4.6. For more information on applying classifications and handling information, refer to Appendix 2, Information Asset Control Measures.

2.5. TOP SECRET Classification

2.5.1. This classification remains for information of the highest sensitivity relating to national security and subject to highly capable threat sources. There is no change to controls at this level. The East Midlands Forces are not expected to generate or handle information at this classification.

2.5.2. For more information on applying classifications and handling information, refer to Appendix 2, Information Asset Control Measures.Midlands Forces

3. Other related documents and appendices

3.1. Appendices.

- Appendix 1 - Government Security Classifications Manual of Guidance
- Appendix 2 – Information Asset Control Measures

4. Monitoring and review

4.1 This policy will be reviewed every two years by the Regional Information Security Officers and Information Managers.

5. Who to contact about this policy

5.1. This policy is owned by Regional Information Assurance Staff. Any enquires about this policy should be directed to Layla Hughes, Vetting & Security Manager, Lincolnshire Police, 07909 687988 layla.hughes@lincs.police.uk.