WARWICKSHIRE POLICE	**POLICY**

Security Classification	Official
Disclosable under Freedom of Information Act 2000	YES

POLICY TITLE	**Information Assurance (Overarching)**
REFERENCE NUMBER	**WP007**
Version	**V2.0**

POLICY OWNERSHIP	
DIRECTORATE	Data, Strategy & Technology
BUSINESS AREA	Information Assurance

INITIAL IMPLEMENTATION DATE	**July 2024**
NEXT REVIEW DATE:	**July 2027**
RISK RATING	**Low**
EQUALITY ANALYSIS	**Low**
TIER	**2**

Warwickshire Police welcome comments and suggestions from the public and staff about the contents and implementation of this policy. Please e-mail policiesandprocedures@warwickshire.police.uk

Contents

1.0 POLICY OUTLINE

Information is an asset which is fundamental to the efficient and effective delivery of policing services. Information comes in many forms, for example, operational data, policy and procedural documents, emails, minutes, statistics, personal data etc. and is held in a variety of manual (hard copy) and electronic formats. Warwickshire Police use information daily as we work to deliver our strategic objectives, and deliver efficient, effective, safe and secure services.

To maximise the benefit of information we need to recognise its value, manage it effectively and ensure that it is adequately protected. Information Assurance (IA) relates to the assessment and management of legal and technical risk relating to the use, processing, storage and transmission of information, and the systems and processes involved in information processing. It encompasses the legal, technical, physical, procedural and personnel controls that address risks to information within an organisation.

This policy sets out the steps that Warwickshire Police will take to assure its information and the systems and infrastructure that support it; by protecting its integrity, availability, authenticity and confidentiality. The policy applies to **all** information held by Warwickshire Police, whether manual or electronic, current or archived and all recorded information, in any form, created, received or maintained by the force. It includes information that supports policing functions as well as administrative functions such as People Services, Business Support, Payroll, Finance etc. The policy also applies to information assets that may be managed or processed by third parties on behalf of Warwickshire Police.

This policy supports the principals of the statutory guidance, issued by the College of Policing, Accredited Professional Practice (APP) – Information Management and the principles detailed in all sections, particularly Information Assurance (IA). It is supported by a number of procedures relating to various aspects of information management to ensure that information is managed legally, securely, effectively and efficiently.

2.0 PURPOSE OF POLICY

The purpose of this policy is to embed information assurance as a core business activity and to ensure that it is considered in the day-to-day management and processing of information. The policy and its associated procedures aim to:

- Recognise the value of information as an asset and ensure that appropriate accountability and controls are in place to protect it.
- Protect the confidentiality, integrity and availability of information assets, whether electronic, paper based or in any other format.
- Ensure that an appropriate governance framework is in place for information management and addressing information risk.

- Ensure that officers, staff, volunteers, third parties and contractors are trained and aware of their responsibilities for managing information.

- Ensure that technology and information systems operate securely and meet His Majesty's Government (HMG) accreditation and information assurance standards, we meet the requirements of the NPCC APPs on Information Assurance, work toward achieving ongoing improvements in or SyAP scores and achieve the Code of Connection requirements for all relevant systems.

- Ensure that Warwickshire Police meet statutory, legal, national and best practices standards for information management.

3.0 IMPLICATIONS OF THE POLICY

3.1 The effective operation of this information assurance policy and associated procedures will support the delivery of effective policing services, enable better business planning, reduce cost and protect people from harm by ensuring that information is secure, accurate and available to the right people at the right time.

This policy and associated procedures support compliance with legal, national and best practice standards including;

- Freedom of Information Act 2000
- Data Protection Act 2018
- UK General Data Protection Regulation (UK GDPR)
- Equalities Act 2010
- Human Rights Act 1998
- Crime and Disorder Act 1998
- Computer Misuse Act 1990
- Official Secrets Act 1989
- Government Security Classifications Policy June 23
- HMG Security Policy Framework Dec 22
- National Police Community Security Policy
- College of Policing Authorised Professional Practice (APP) – Information Management and its principles including Information Assurance (IA), Management of Police Information (MoPI)
- International Organisation for Standardisation (ISO) 27001:2013 Information Security Management
- British Standard (BS) 10008:2008 Evidential weight and legal admissibility of electronic information.

Failure to comply with the policy could result in impact on:

- Legal compliance
    - Breach of Data Protection Act 2018 or other applicable law
- Finance
    - GDPR fines of up to 20 million euros (circa 16 million pounds) or 4% of turnover for personal data breaches.
    - Cost of managing, investigating and recovering from incidents.
- Personal

    - Risk of harm to individuals if information is subject to unauthorised disclosure, inaccurate, or unavailable.
- Reputation
    - Loss of reputation and public confidence in the police
- Operational
    - Inability to deliver services if information is not available to the right people and/ or cannot be relied upon as accurate.
- Government/ Policing Standards
    - Failure to meet HMG standards for connection to Public Service Network (PSN), PDS SyAP and National Systems (which may result in increased costs and operational impact).

4.0 POLICY STATEMENT

Good information assurance requires clear and effective management and accountability structures, assurance processes, documented policies and procedures, trained staff and adequate resources.

4.1 Information Assurance Management and Governance

Warwickshire Police must have clear lines of accountability for information assurance, with key roles in place based on the Cabinet Office Information Risk Framework, and information assurance monitored and managed through the appropriate governance groups.

Appendix A outlines the key roles and responsibilities for information assurance.

Appendix B outlines the governance groups in place for information assurance

4.2 Risk management

Processes must be in place for managing risk that reflect business objectives to support good risk management. This includes assessments to identify potential threats, vulnerabilities and appropriate controls to reduce risks to people, information and infrastructure, with assurance processes to ensure that mitigations are effective. These risks are managed through DPIAs and IRARs and surfaced through the IA Risk Register which supports the Force Level Information Assurance risk.

4.3 Information

Mechanisms and processes must be in place to ensure assets are properly classified and appropriately protected, and there is confidence that systems and services can protect the information that they carry.

4.4 Technology and Services

Procedures must be in place to protect against, detect and correct malicious behaviour. Critical technology and services will be resilient to cyber incidents and have the means to recover from these.

4.5 Personnel Security

Processes must be in place for pre-employment vetting checks and ongoing security management of people with access to information, with regular monitoring and assurance, to mitigate insider risk.

4.6 Physical security

Processes and plans must in place to determine and implement appropriate physical security controls for information assets based on their criticality and sensitivity.

4.7 Information Security Incident Procedures

Processes must be in place for reporting, managing and resolving any security incidents. This includes ensuring organisational learning from incidents. Business continuity arrangements must ensure resilience and ensure quick and effective recovery from incidents.

4.8 Training and Awareness

All officers, staff, volunteers, third parties and contractors must be aware of their own personal responsibilities for managing information and undertake the appropriate training in line with National Police Chiefs' Council (NPCC) requirements.

This includes the completion of the relevant College of Policing Managing Information courses, and additional specialist training for specific job roles:

	Managing Information- Relevant module **(Operational/ Non-Operational)**	**Protecting Information- Level Two**	**Protecting Information- Level Three**	**Data Protection Foundation Level** **Mandatory for all new starters**
All officers, staff, contractors, volunteers	Mandatory			Recommended as supplementary
Senior Information Risk Owner (SIRO)	Mandatory	Recommended	Recommended	Recommended as supplementary
Senior Information Asset Owner/Information Asset Owners	Mandatory	Mandatory	Recommended	Recommended as supplementary
Information Asset Owners Nominated Officers	Mandatory	Recommended	Recommended	Recommended as supplementary
Data Protection Officer	Mandatory	Recommended	Recommended	Recommended as supplementary

The Information Assurance Team are implementing a range of bespoke and Face to Face training to support Data Protection awareness in collaboration with Learning & Development.

‘Any individual who fails to complete mandatory training and pass the associated competency tests should be given time to re-sit the training and pass the test. The individuals line manager / supervisor will decide whether the individual requires additional training prior to re-sitting the test. Any individual who fails a second time should be given one-to-one instruction under arrangements made by their line manager / supervisor.

5.0 PROCEDURE

This is the overarching policy for information assurance. This, and its supporting procedures are aligned to HMG Security Policy Framework and recognised standards that Government and Public Sector bodies adhere to for information assurance. Procedures that are currently in place to support this policy include:

- **Personnel Security Procedure**
  This sets out the requirements in relation to the vetting of all Force personnel - and those of third party suppliers, contractors and Partner Agencies - who have access to the Forces’ information assets or the equipment on which they are processed.

- **Clear Desk and Clear Screen Procedure**
  This informs all members of the Force and OPCC and occupants of police premises - and those that police share with others - how information assets should be securely stored when not in use. It also advises how unauthorised access to displayed information assets should be prevented.

- **Information Classification Procedure**
  This sets out how the Force will implement their chosen valuation and Marking scheme for their information assets - the Government Security Classification (GSC) scheme.

- **Accreditation Procedure**
  This sets out the methodology and process for the proportionate accreditation (including initial risk assessment) of any information processing system.
  A Risk Management & Accreditation Document Set (RMADS) may be required to be produced as part of the accreditation process.

- **User Account Management Procedure**
  This sets out the requirements for the secure management of such accounts and their access credentials (e.g. passcodes or Smartcards) once issued. This includes the deletion and disabling of accounts and/or access credentials.

- **Passcode Management Procedure**
  This sets out how system passcodes are to be set and reviewed; including the expected complexity for their formation, frequency of passcode changes and security once issued.

- **Information Security Incident Management Procedure**
  This sets out the process for the reporting, and subsequent investigation, of

deliberate, accidental or potential security incidents involving the Force and OPCC information assets and premises (whether or not shared with others).

- **Secure Sanitisation and Disposal Procedure (ICT Owned)**
  This describes how the Force and OPCC ensure that redundant information assets and any equipment on which they have been processed, should be disposed of, to prevent such data being accessed inappropriately.

- **Protective Monitoring Procedure (ICT Owned)**
  This describes the process by which ICT system activity is logged in order to provide an audit trail of security events of interest and when and how such data is subsequently used.

- **Lockdown Procedure (ICT Owned)**
  This describes that part of the proportionate suite of technical countermeasures that includes content lockdown to restrict the availability and use of unnecessary services.

- **Off-Site Security of Police Information and Equipment Procedure**
  This sets out the security countermeasures to reduce the risks of compromise of the Forces' information, and information-processing, assets to an acceptable level when they are not on secured Police Premises.

5.0 DOCUMENT HISTORY

Date	Author / Reviewer	Amendment(s) & Rationale	Date of Approval / Adoption
Dec 2018	A Baylis	Previously Approved at Alliance JNCC	JNCC11/12/2018
Nov 2019	E Peberdy	Reviewed – Updated to Warwickshire Policy mandatory	Nov 2019
Feb 2024	Sara Smith	Reviewed. WKP template update. Minor wording changes to reflect WKP practice	July 2024

6.0 CONSULTATION

6.1 IA Team/Critical Friends/IAB Group

7.0 ASSESSMENT AND ANALYSIS

7.1 Completed and available on request.

Appendix A – List of Key Roles & Responsibilities

SIRO

The Deputy Chief Constable has been nominated as Senior Information Risk Owner (SIRO)
The responsibilities of the SIRO are:

• Take overall ownership of the organisation's Information Risk Policy
• Understand how the strategic goals of the Force may be impacted by information risks, and how those risks may be managed
• Have oversight and direction for the Information Assurance function.
• Sign off and take accountability for high rated risk-based decisions and reviews in regards to the processing of Force data
• Advise the Senior Leadership on the effectiveness of information assurance and risk management across the Force
• Receive training as necessary to ensure they remain effective in their role as SIRO.

Data Protection Officer

The Head of Information Assurance is the DPO who reports to the SIRO both directly on operational matters and also through the Director, Data, Strategy & Technology
The DPO can also act independently of the SIRO and report directly to Senior Leadership about significant data protection matters.
These may include information assurance risks to the organisation, privacy concerns or recommendations with regard to potential changes to, or new initiatives that involve processing of personal data.

With the support of their Team, the DPO will:

• provide advice to the organisation and its employees on compliance obligations with data protection law
• advise on when data protection impact assessments are required
• monitor compliance with data protection law and organisational policies in relation to data protection law
• co-operate with, and be the first point of contact for the Information Commissioner
• be the first point of contact within the organisation for all data protection matters

Information Assurance Team

The team comprises the Senior Information Assurance Officer, Data Protection Adviser, Information Security & Assurance Officer, Records and Data Quality Manager
Records Review and Disposal Officers.
The team supports the implementation of IA policies, procedures, training and awareness, the management of incidents, data quality issues and the records retention schedule.

Information Asset Owners

Information Asset Owners (IAOs) will:

• Lead and foster a culture that values, protects and uses information for the benefit of the Force and the public
• Know what information comprises or is associated with their asset(s) and understand the nature and justification of information flows to and from the asset
• Know who has access to the asset, whether system or information, and why, and ensure access is monitored and compliant with policy
• Understand and address risks to the asset and provide assurance to the SIRO
• Ensure there is a legal basis for processing and for any disclosures, and
• Refer queries about any of the above to the Information Assurance team
• Ensure all information assets they are owner for are recorded on an Information Asset register and are maintained
• Undertake specialist information asset owner training as required.

Information Asset Nominated Officers
Support IAOs in the day-to-day operational management of the assets identified and may take on delegated responsibility from the IAO's as appropriate.

Appendix B – Governance Reporting