

 WARWICKSHIRE POLICE		POLICY
Security Classification	OFFICIAL	
Disclosable under Freedom of Information Act 2000	YES	

POLICY TITLE	Protective Monitoring
REFERENCE NUMBER	WP066
Version	1.0

POLICY OWNERSHIP	
DIRECTORATE	Data, Strategy and Technology
BUSINESS AREA	Digital Services

INITIAL IMPLEMENTATION DATE	10/09/2025
NEXT REVIEW DATE:	10/09/2027
RISK RATING	MEDIUM
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 PAGE:

1.0	POLICY OUTLINE
2.0	PURPOSE OF POLICY
3.0	IMPLICATIONS of the POLICY
4.0	PROCEDURE
5.0	DOCUMENT HISTORY
6.0	CONSULTATION
7.0	ASSESSMENT AND ANALYSIS

1.0 POLICY OUTLINE

- 1.1 Warwickshire Police (The Force) have an obligation to ensure that its information and assets are protected from any breach of confidentiality, integrity, and availability by providing sufficient monitoring of its digital estate.
- 1.2 In this policy 'Staff' refers to all Police Officers, Police Community Support Officers (PCSOs) and Special Constables, Police Staff, Office of the Police & Crime Commissioner (OPCC) staff, volunteers, contractors, temporary and agency workers.
- 1.3 It is a requirement of Police Digital Services for forces enrolled in their National Management Centre protective monitoring to provide adequate logs, known as A-N requirements.
- 1.4 It is a requirement of the national SyAP (Formally known as the GIRR) for Forces to have adequate logging, audit and monitoring capabilities as part of the "detect" controls that form part of national accreditation.

2.0 PURPOSE OF POLICY

Protective Monitoring is essential to enable the Force to prevent cyber security incidents as well as detecting ongoing ones at the earliest stage to limit the blast radius of an incident. It also provides forensic data for analysis in the event of a cyber incident which can be used as part of a criminal investigation by the Force's Cyber Crime team alongside national partners such as the NMC, NCSC and NCA.

This policy is required to ensure that Warwickshire Police are compliant with PSN/PSN-P national accreditation as well as conforming to several areas of the National Policing SyAP in which all forces must achieve at least a minimum baseline score to remain compliant and access national applications.

The policy ensures that Warwickshire Police meet the requirements of the National Monitoring Centre.

The policy replaces a legacy policy that was first implemented in 2016 (A022j) that referred to legacy national standards/frameworks and accreditation.

3.0 IMPLICATIONS of the POLICY

- 3.1 Adequate financial provisions should be made available to ensure that the provision of protective monitoring is available to the force 24/7/365.
- 3.2 Digital Services staff must be trained on using the protective monitoring solution in place.

- 3.3 All protective monitoring data will be held in UK PASF assured data centres and conform to UK GDPR.

4.0 PROCEDURE

- 4.1 Warwickshire Police will conform to the requirements laid out to forces in the National Enabling Programme blueprints in relation to Protective Monitoring as detailed in the Warwickshire Police Protective Monitoring Procedure
- 4.2 Warwickshire Police will respond to alerts and intelligence gathered through the use of Protective monitoring as per the Warwickshire Police Threat Intelligence Procedure.
- 4.3 It is the responsibility of Digital Services to ensure that Warwickshire Police remain compliant with national standards in these areas.
- 4.4 ***Please state which head of department or chief officer has been consulted in the development of this policy:***

<i>Head of Dep't/ Chief Officer Consulted</i>	<i>Date Communication Sent</i>
<i>Steve Maxwell – Head of Digital Services</i>	<i>12/12/2024</i>

5.0 DOCUMENT HISTORY

The history and rationale for change to policy will be recorded using the below chart: If you are using this template for a review of a harmonised policy **you must** state in the amendment(s) section what you have changed and complete a Summary of Change form, (please request from Policy Team).

Date	Author / Reviewer	Amendment(s) & Rationale	Date of Approval / Adoption
12/12/2024	J Morgan-Jones	New policy to replace A022j). Policy has been completely overhauled due to changes in Force and National structures and accreditation.	
10/06/2025	J Morgan-Jones	Updated to Production	16/06/2025 Governance Board Published 10/09/2025

6.0 CONSULTATION

6.1 Director of Data, Strategy and Technology
Head of DS
Head of IA
Head of Service Management
Cyber Security Architect
Infrastructure Architect
Network Architect
Critical Friends

6.2 The above parties have reviewed this Policy and associated procedures.

7.0 ASSESSMENT AND ANALYSIS

The Equality Analysis (EA), Health & Safety Assessment (HAS) and Risk Assessment (RA) associated with this document are available on request.