West Mercia POLICE		POLICY
Security Classification	**OFFICIAL**	
Disclosable under Freedom of Information Act 2000	Yes	

POLICY TITLE	**Intelligence Access Levels**
REFERENCE NUMBER	**WMP185**
Version	**1.0**

POLICY OWNERSHIP	
DIRECTORATE	CRIME & VULNERABILITY
BUSINESS AREA	INTELLIGENCE

INITIAL IMPLEMENTATION DATE	**February 2022**
NEXT REVIEW DATE:	**February 2025**
RISK RATING	**LOW**
EQUALITY ANALYSIS	**LOW**

West Mercia Police welcome comments and suggestions from the public and staff about the contents and implementation of this policy.
Please e-mail contactus@westmercia.pnn.police.uk

1.0 POLICY OUTLINE

This procedure provides a framework for the management and operation of Intelligence access levels within the West Mercia Police Intelligence system, ATHENA / GENIE. This will outline the current Intelligence system access structure and identify key staff and their roles and responsibilities in relation to the management of access levels.

The framework is limited to the consideration of Intelligence access levels which require restriction due to the nature of the Intelligence which they hold. Thus, it will be restricted to the management of Intelligence access levels of 5, 15 and 99. Within West Mercia the Intelligence levels are identified as follows:

- Level 5 – Highest level of Intelligence with access restricted to a small number of individuals with specialised Intelligence roles
- Level 15 – Medium level of Intelligence with access restricted to staff engaged in the submission, handling and management of Intelligence in connection with Force level operations or of a particularly sensitive nature
- Level 99 – General access is for those of whom who would be expected to submit Intelligence reports

Acknowledgement is made of the 'Need to Know' principle and access should be granted at a level appropriate to an individual's job functions and the minimum required for carrying out such functions, which this procedure will outline.

ATHENA is the primary West Mercia Intelligence system and the mechanism for controlling access to Intelligence. The access applied to this system must be carried across to any other IT system which allows access to Intelligence information e.g. GENIE.

2.0 PURPOSE OF POLICY

The purpose of this policy is to provide information / detail relating to the following:

- Ensure that only the correct staff have elevated access levels, to protect the integrity of intelligence in relation to more sensitive operations or investigations.
- Ensure appropriate access to restricted Intelligence, of which is graded at a level 5 or 15, is only available on a 'Need to Know' basis and to ensure that this is managed effectively. This includes the adding and removing of these permissions based upon a Role Based Access approach.
- Ensure, and provide information around the correct access of intelligence dependent upon the Handling, Action and Sanitising Codes that are applied to Intelligence records held within West Mercia Police.
- Which teams should have what access level and permission bundles within the intelligence system(s)
- The onus is on teams or individuals, who seek a higher access, to identify what level and permission bundle they need and to relay that rationale, and ensure that they have the correct vetting level of Management Vetting with Security Clearance (MVSC). If granted, they must also later request that the higher

graded access is removed, if it is no longer required i.e. they have moved to a role where the higher level access is not needed.

3.0 IMPLICATIONS of the POLICY

The Police collect information that is required for policing purposes. Policing purposes provide the legal basis for the collection, recording, evaluation, sharing and retention of information and may include one, or a combination, of the following:

- Protecting life and property
- Preserving order
- Preventing the commission of offences
- Bringing offenders to justice
- Any duty or responsibility arising from common or stature law

Handling codes are a control mechanism for Intelligence sharing. The risks associated with sharing Intelligence must always be weighed against the potentially greater risk of not sharing. Handling codes are supported by conditions for Intelligence sharing.

Before disseminating intelligence, the person disseminating should ensure they are familiar with the appropriate legislation and their organisation's policies, standards and operating procedures and other frameworks.

In order to share this Intelligence there must be:

- A policing purpose
- A legitimate need to receive it

Lawful policing purposes are defined as:

- Protect life and / or property
- Preserve order
- Prevent the commission of offences
- Bring offenders to justice
- Linked to any duty or responsibility arising from common or stature law

Specific questions need to be asked when considering dissemination of code P intelligence. For example:

- Are there legal obligations?
- Who is asking for it?
- Why do they want it?
- What are they going to do with it?

Intelligence sharing should be proportionate and carried out in accordance with principles of the Human Rights Act 1998.

4.0 PROCEDURE

A Standard Operating Procedure in support of this policy has been created and is not for public dissemination.

5.0 CONSULTATION

Business Lead/ Chief Officer Consulted	***Date Consulted***
Supt Intelligence/ ACC C&V	November 2021

Key stakeholders consulted in the development of this policy include:

- Detective Inspector FIB
- Detective Inspector Field Intelligence – North
- Detective Inspector Field Intelligence – South
- Manager IPU and PNSB
- Business Systems Administration Manager
- Miss Natalie Vale – IPU Manager
- Mr Adam Lowe – Business Systems Administration Manager
- Critical Friends Group

6.0 DOCUMENT HISTORY

The history and rationale for change to policy will be recorded using the below chart:

Date	**Author / Reviewer**	**Amendment(s) & Rationale**	**Date of Approval / Adoption**
Nov 2021	S Fitzpatrick	New Policy and Procedure	JNCC Exec Board 08/02/2022

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.

8.0 DATA PROTECTION IMPACT ASSESSMENT

- Is a DPIA required? – No, agreed by Audit, Risk and Compliance on 8th November 2021

9.0 MONITORING / EVALUATION

The Monitoring and review of this policy is the responsibility of the policy owner.