Gloucestershire Constabulary
Police Headquarters
No.1 Waterwells, Waterwells Drive
Quedgeley, Gloucester. GL2 2AN
www.gloucestershire.police.uk

Your reference:
Our reference: FOI_24_0668
E-mail: FOI @gloucestershire.police.uk
Direct dial: 01452 754304
Postal Address: As above
Date: 14/05/2026

Dear

Gloucestershire Constabulary Freedom of Information request FOI_24_0668

On 14/07/2024 you sent an email constituting a request under the Freedom of Information Act asking the following:

1) The College of Policing requirements for Information Management specify that each UK police force must have an Information Management Strategy (IMS): https://www.college.police.uk/app/information-management/management-police-information/common-process-managing-police-information#information-management-strategy
Please provide a copy of your local Police Force's IMS.

2) Please provide your Policy relating to the Management of Intelligence. As an example, I have attached Surrey's and Sussex's Policy.

3) Do you use the same system for crime and intelligence recording? What are the name(s) of the system?

4) In accordance with the National Intelligence Model, all intelligence should be handled using the 3x5x2 grading system, in which three source gradings exist; Reliable, Untested and Unreliable. In order to supplement National documents, an example of which I have attached and information available from National Policing College, via weblink: https://www.college.police.uk/app/intelligence-management/intelligence-report — what internal written material on the subject of intelligence has been produced by your Police Force (i.e. Guidance/a Handbook/Aide Memoire/Page on your Intranet or similar in nature) and is available to assist your officers? Please provide a copy of the information

Under the Freedom of Information Act 2000 s1, I can confirm that Gloucestershire Constabulary holds some relevant information.

Q1. Please see the attached document:

- FOI_24_0668 - Information Management Strategy - Version 1.7 2021_Redacted

The redacted information is subject to S.40 exemptions.

Q2. Please see the attached document:

- FOI_24_0668 - Intelligence guidance document_Redacted

The redacted information is subject to S.31 exemptions.

Q3. Unifi. This is correct as at the time of the request.
Q4. Please see Q2.

Section 17 of the Freedom of Information Act 2000 requires Gloucestershire Constabulary, when refusing to provide information (because the information is exempt) to provide you the applicant with a notice which: (a) states the fact, (b) specifies the exemption in question and (c) states (if not otherwise apparent) why the exemption applies.

Regarding the redacted information, the following exemptions apply:

Section 31(1)(a) – Law Enforcement
Section 40(2) – Personal Information

Section 31 exemption is qualified and prejudice based therefore both a Public Interest Test and Harm Test are required.

Section 40(2) applies to third party personal data. This would not be released under the Freedom of Information Act unless there is a strong public interest. The disclosure of any information which could lead to the identification of an individual would breach the Data Protection Principles contained with the Data Protection Act 2018, namely the first principle which states that personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.

This exemption is absolute and class based therefore I am not required to apply either the public interest test or harm test in disclosure.

In accordance with the Act, this letter represents a Refusal Notice for this part of your request.

Section 31
Evidence of Harm

Release via the Freedom of Information Act is deemed a release into the public domain.

To provide details of how the police record and use intelligence, may allow offenders to change their behaviour in a detrimental way.
The disclosure of information which is likely to undermine the Constabulary's ability to serve the public in preventing and detecting crime can only be considered as being harmful to the public.

Public Interest Test

Factors in Favour of Disclosure

Disclosing policies used by Police would provide a greater transparency in their actions and ensure that they operate effectively and efficiently.

Factors against Disclosure

Releasing the policy to the public could share strategies used by Gloucestershire Constabulary to conduct investigative work and could reduce the ability of the Police to prevent and detect offences and apprehend offenders.

Balance Test

The Police Service is charged with enforcing the law, preventing and detecting crime and protecting the communities we serve. Whilst there is a public interest in the transparency of policing procedures, there is a very strong public interest in safeguarding tactics and capabilities to ensure that the protection of the public is safeguarded. Therefore, it is our opinion that the balance of the public interest favours withholding the information.

In accordance with the Act, this letter represents a Refusal Notice for this part of your request.

If you are not satisfied with this response or any actions taken in dealing with your request, you have the right to ask that we review your case under our internal procedure. Please note that a request for an internal review must be made within 20 working days of the response to your original request.

If you decide to request that such a review is undertaken and following this process you are still unsatisfied, you then have the right to direct your complaint to the Information Commissioner for consideration.

The Information Commissioner can be contacted via the following means:

Website - https://ico.org.uk/
Call their helpline - 0303 123 1113
Email - casework@ico.org.uk
Post – Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Yours sincerely,

Disclosure Officer
Gloucestershire Constabulary

Information management strategy

Origin/Author : G &C SMT

Sponsored by : [redacted]

Date Approved : April 2017

Reviewed : February 2021

Version 1.2

Contents

Introduction

The Gloucestershire Constabulary Information Management Strategy (IMS) will apply to all Constabulary information collected, received, created, held, shared, disseminated, disclosed, maintained, reviewed, retained or disposed of by all staff and officers employed by the Force in the course of carrying out their duties. This document covers all formats of information including, but not limited to, electronic, digital and hard copy.

It is intended that the Gloucestershire Information Management Strategy (IMS) will provide the foundation for the iterative development of how we professionalise the management of information in the Constabulary. Information is the Constabulary's most valuable asset and without it the force will be unable to achieve its visions or strategic aims.

The Strategy will set out the key principles of information management. The Information Management Policy will detail the underlying standards, roles and responsibilities of key personnel in the management of information. It is the responsibility of everyone within the Constabulary to ensure information is used appropriately, in line with this strategy and accompanying policies and procedures.

Gloucestershire Constabulary has a corporate responsibility to manage all information received, created and held for a policing purpose. The person with overall responsibility for this strategy is the Chief Constable.

The Information management strategy sets out how the Force will work within a regulatory environment complying with relevant and related legislation, statutory instruments, Common Law and Codes of Practice (appendix A)

Who is responsible for police information held within the force; also known as the Data Controller.

The purposes for collecting and holding information.

Which processes ensure that police information is audited for accuracy and relevance to the policing purposes?

The controls that are applied to ensure the integrity and security of police information held by the force.

The training required to support the management of police information.

The dedicated resources which support the delivery of the IMS and their relationship to other business areas.

Arrangements for receiving records and monitoring record keeping.

How the force complies with national and local security policy and standards

1. Strategic objectives and alignment

The Chief Constable is also the Data Controller (DC). This role is defined in the Data Protection Act 1998 as the individual within an organisation who determines the purpose and manner in which personal data is processed.

The Head of Governance and Compliance will be responsible for overseeing the IMS to ensure that information management policies, processes and procedures are followed, risks mitigated, quality standards met and benefits realised.

With the support of the Governance and Compliance Senior Management Team, which includes the following business areas:

- Audit and Compliance
- Information Disclosure – Data Protection, Freedom of Information, Information Sharing, CICA.
- Risk Management and Insurance
- Information Security
- Records Management
- Unifi and PNC support
- Data Quality
- Disclosure and Barring

The force has produced policies to help implement the IMS approach (appendix B).

The IMS will provide a framework around managing the Constabulary information throughout its lifecycle and to give a focus which has been missing. It aligns with all force strategic objectives within the Corporate Strategy:

This also aligns to the OPCC Police and Crime plan.

2. Information Management Strategy - Objectives

- Define, support and develop Information Asset Owners (IAO) and their roles and responsibilities.
- Develop guidance and introduce the Government Security Classification (GSC) and maintain compliance with the force's GSC policy.
- Align with force programmes, including the Digital Transformational Programme ensuring a consistent approach and delivery of information management is achieved.
- To ensure that force align to the Data quality principles as set out by the College of Policing: http://www.app.college.police.uk/app-content/information-management/management-of-police-information/collection-and-recording/#data-quality-principles
- Develop and introduce information management compliant systems and assets.
- Align to the GDPR Data Protection Act 2018 and the new European Data Protection Regulations.
- Ensure compliance with the Freedom of Information Act 2000.
- To ensure that the Constabulary aligns with Management of Police Information (MOPI) as set out by the College of Policing.

3. Key roles and responsibilities

In Gloucestershire we have a corporate responsibility to own and manage all information received, created and held for a policing purpose in accordance with the regulatory environment. The person with overall responsibility for this strategy is the Chief Constable.

The Chief Constable is also the data controller. This role is defined in the Data Protection Act 2018 as the individual within an organisation who determines the purpose and manner in which personal data is processed.

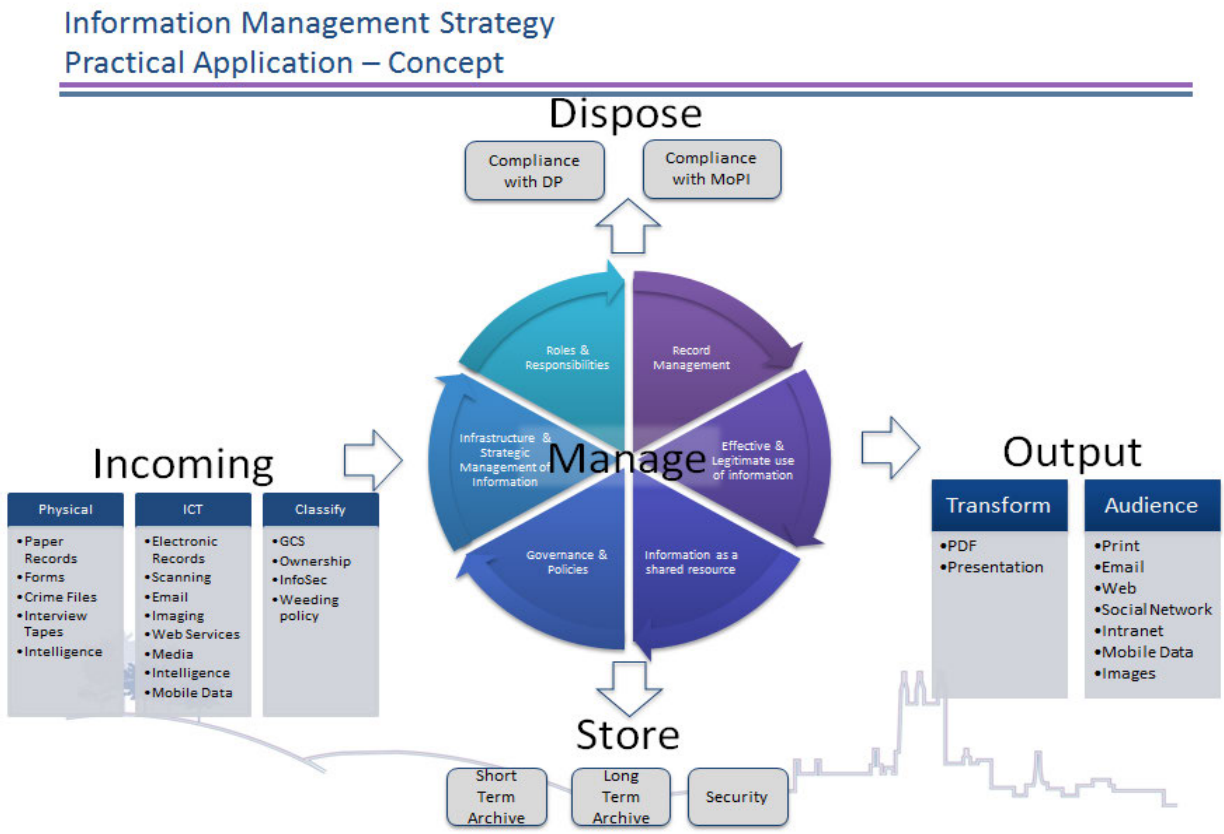
The Head of Governance and Compliance will be responsible for overseeing Information Management to ensure that information management policies, processes and procedures are followed, risks mitigated, quality standards met and benefits realised.

The force has a corporate responsibility to ensure it has a business continuity plan in place to safeguard its corporate and information assets.

The force will adopt the named responsibilities identified in MOPI People Assets.

All staff within the Force will ensure that all information created, received and held, for which they are responsible, is accurate, relevant and kept up to date. This strategy will be made available to our partners and the public.

4. Role alignment within the Strategy



All staff within the Force will ensure that all information created, reviewed and held for which they are responsible is accurate, relevant and kept up to date. All staff will:

- Apply the basic principles of effective information management as contained in Authorised Professional Practice
  Apply the data quality principles to all police information
  Apply the operating rules relevant to the business areas to which they have access Apply the rules relating to information security
- Ensure compliance with all relevant legislation, including the Human Rights Act 2018, Data Protection Act 2018 and Freedom of Information Act 2000
- To complete all relevant training to support this strategy and the management of police information.
-

5. Benefits of having an Information Management Strategy

Strategic Benefits	Tactical Benefits	Operational Benefits
IMPROVED POLICE PERFORMANCE	Nationally consistent and effective management of information Improved auditing of decision-making process Increased understanding of and compliance with relevant legislation Reduced civil actions and complaints against forces as a result of poor information management.	Improved data quality Responsibilities in relation to information management are clear Less officer/staff time and effort is needed to access information Less impact of civil action and formal complaints on officer/staff time and wellbeing.
SAFER COMMUNITIES	More informed decision making Improved targeting Improved processes for joint agency working Effective management of high risk offenders Enhanced disclosure processes Improved protection of children and vulnerable adults	Related information is linked and associations between crime and offenders are more easily made Better deployment of operational resources Increased willingness of partner agencies to share information Less bureaucratic processes for sharing information
INCREASED PUBLIC CONFIDENCE	Improved victim/witness satisfaction Improved community relations	Increased reporting of crime Increased provision of community intelligence

Appendix A

Strategic Drivers

The strategy holds regard to the following regulators and national bodies that develop and oversee standards, these strategy key points are detailed below:

Her Majesty's Inspectorate of Constabulary (HMIC)
Independently assesses police forces and policing across activity from neighbourhood teams to serious crime and the fight against terrorism-in the public interest.

2015 Principal Inspection Objectives:

- If Force strategies, policies & procedures for information management adhere to the principles of the APP on information management and former editions of the national guidance, are proportionate to risk and fit for proper use.
- If information & intelligence are captured, recorded, evaluated, acted upon, audited and retained by police (including safeguarding interventions) in an effective way; and
- If the use of the Police National Database is effective and efficient

Information Commissioner's Office (ICO)
The ICO is the independent regulatory office dealing with the Data Protection Act 1998 and the Freedom of Information Act 2000.

Data Protection Principles:
Everyone responsible for using data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly and lawfully
- used for limited, specifically stated purposes
- used in a way that is adequate, relevant and not excessive
- accurate
- kept for no longer than is absolutely necessary
- handled according to people's data protection rights
- kept safe and secure
- not transferred outside the European Economic Area without adequate protection

Freedom of Information Act:

- Everybody has a right to access official information. Disclosure of information should be the default – in other words, information should be kept private only when there is a good reason and it is permitted by the Act;

- An applicant (requester) does not need to give you a reason for wanting the information. On the contrary, you must justify refusing them information;

- You must treat all requests for information equally, except under some circumstances relating to vexatious requests and personal data. The information someone can get under the Act should not be affected by who they are. You

should treat all requesters equally, whether they are journalists, local residents, public authority employees, or foreign researchers; and

- Because you should treat all requesters equally, you should only disclose information under the Act if you would disclose it to anyone else who asked. In other words, you should consider any information you release under the Act as if it were being released to the world at large

Home Office
Code of Practice on the Management of Police Information (2005)
Key Principles Governing the Management of Police Information Principles:

- Duty to obtain & manage information
- Requirement for police information
- Grading & recording of police information
- Ownership of police information
- Review of police information
- Retention and disposal of police information
- Sharing of police information within the UK police service
- Sharing of police information outside the UK police service
- Protection of sensitive police information and sources
- Obligations of those receiving police information

National Intelligence Model Code of Practice

NIM depends on information to feed the intelligence process.

The purpose of this code is:

- To set out to chief officers of police the basic principles and minimum common standards for the National Intelligence Model
- To promote **compatibility** of procedures and of terminology for the National Intelligence Model
- To clarify the **responsibilities** of chief officers and of police authorities in relation to the application of the National Intelligence Model
- To ensure that observance of these principles, and the standards for implementation, results in a systematic programme of continuous development of police policy, practice and capability To identify and promulgate good practice.

Appendix B

Force Policies

The Information Governance Board is responsible for strategic ownership and annual review of the following Constabulary policies and procedural documents:

- Archive
- Data Protection
- E-Mail Security
- Force Vetting
- Freedom of Information
- Government Protective Marking Scheme
- ID Cards
- Information Security
- Information Sharing
- Internet Security
- Network Security
- Patch management
- Records Management
- Visitor Policy

All policies are available on the Constabulary's intranet, the G&C administrator is the force contact for all policies.

Appendix C

The Transformation Programme

The Transformation Programme has a number of objectives; four of these apply to the IMS:

- Increase efficiency and reduce costs through digitally enabled process improvement & innovation in the way we work
- Improve the capability for officers and staff to work more effectively, by providing the right tools to enable access to information where and when they need it
- Increase the ease and effectiveness of work with partners, provide flexibility to reshape and interoperate, through enhanced mechanisms to share information
- Increase the ability to exploit information and intelligence to inform decisions, investigations, management of threat and the deployment of resource.
- Take into consideration Data quality when supporting the development or transition of force system.

Document Control

Version History

Version	***Date***	***Comments***
		First draft prepared by
1.0	02/11/2016	[redacted]
1.2	16/11/2016	G&C SMT
1.3	11 April 2017 August 2019 February 2021	[redacted] G&C G&C SLT

Document Distribution

Name	***Location***	***Responsibility***	***Action/Inform***
			A
			I
			I
			I

Document Reviewed By

Name	***Location***	***Responsibility***
[redacted]	**G&C kdrive**	

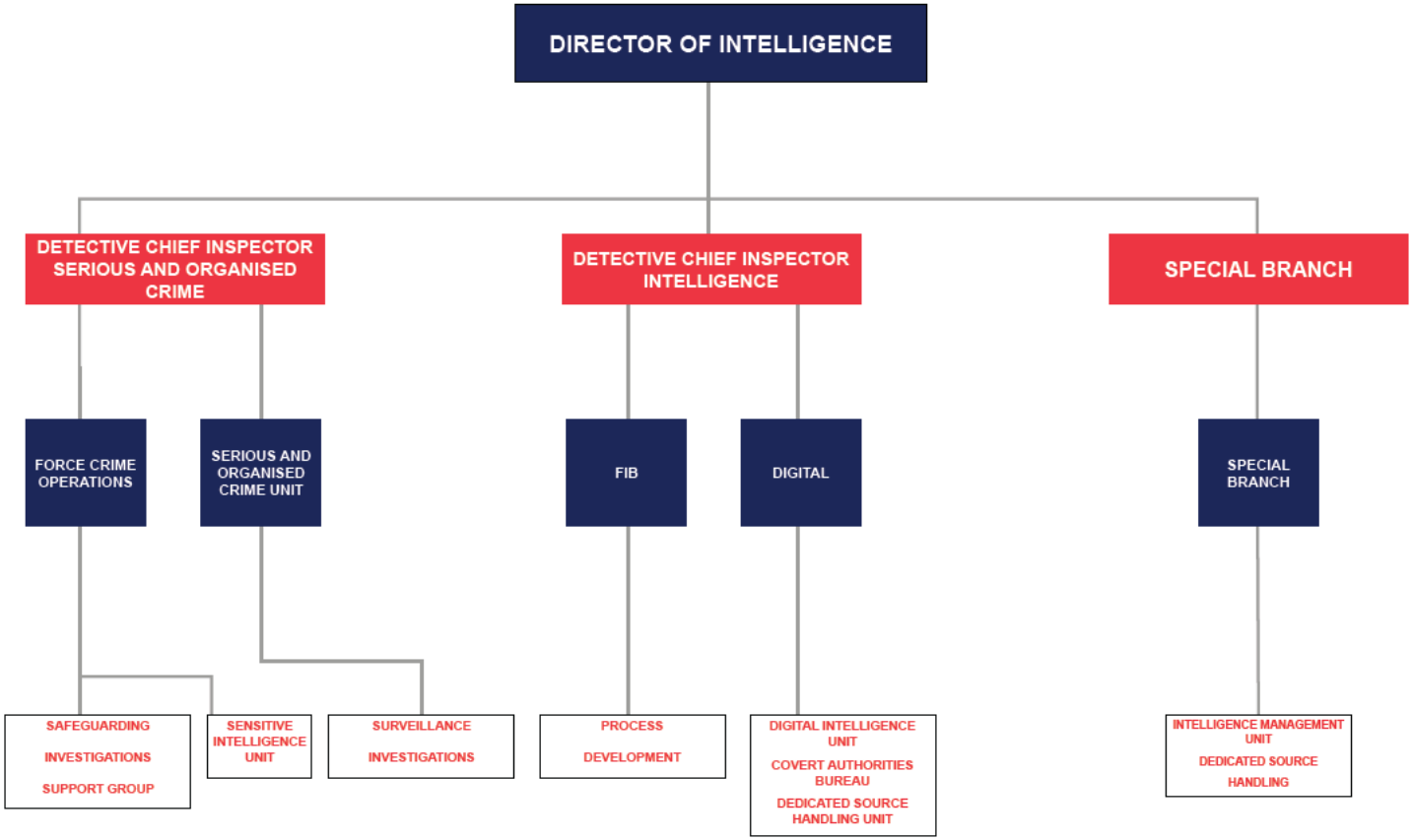
Gloucestershire Constabulary

Intelligence guidance

June 2019

Contents

Intelligence Department



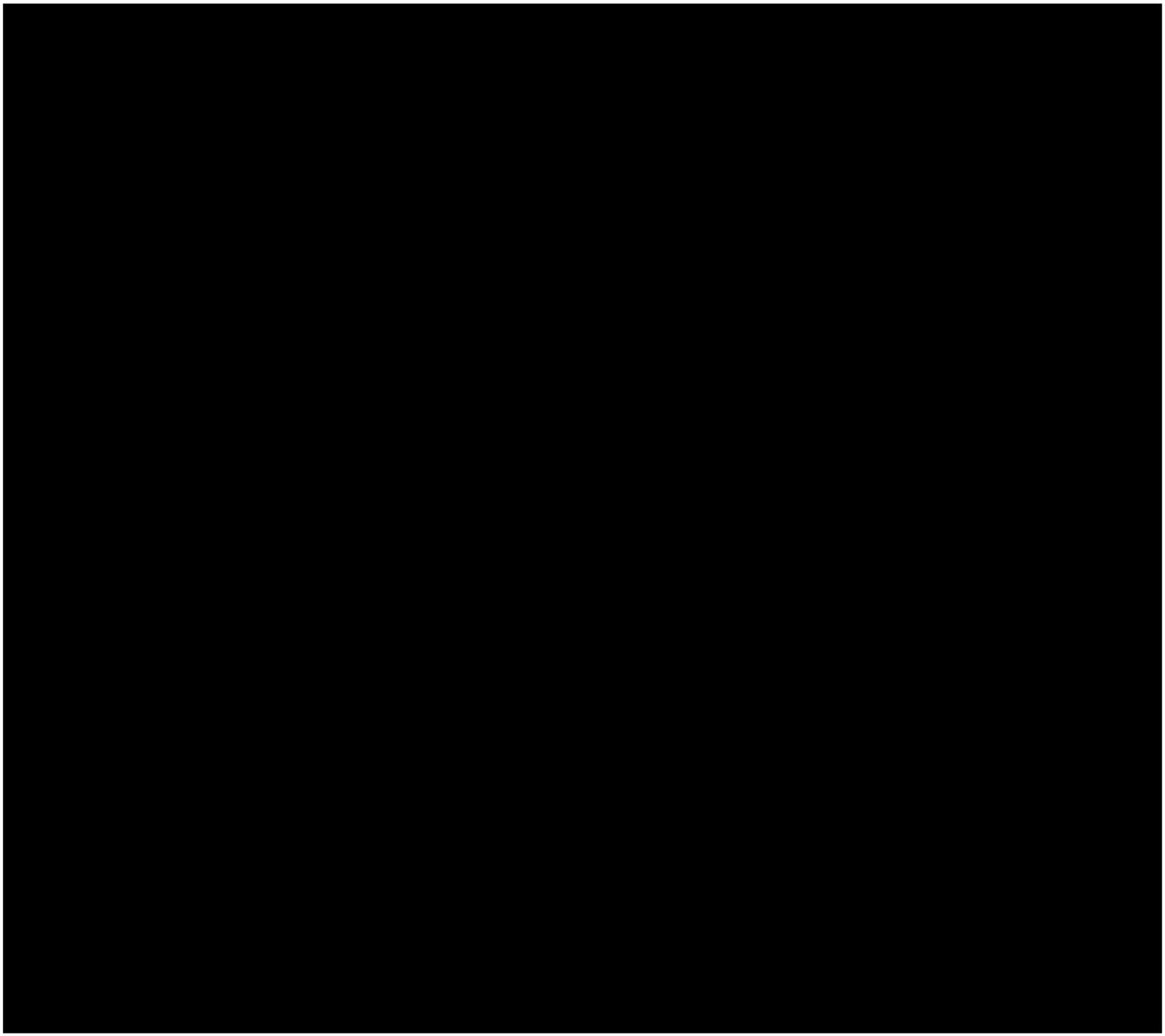
[redacted]

[redacted]

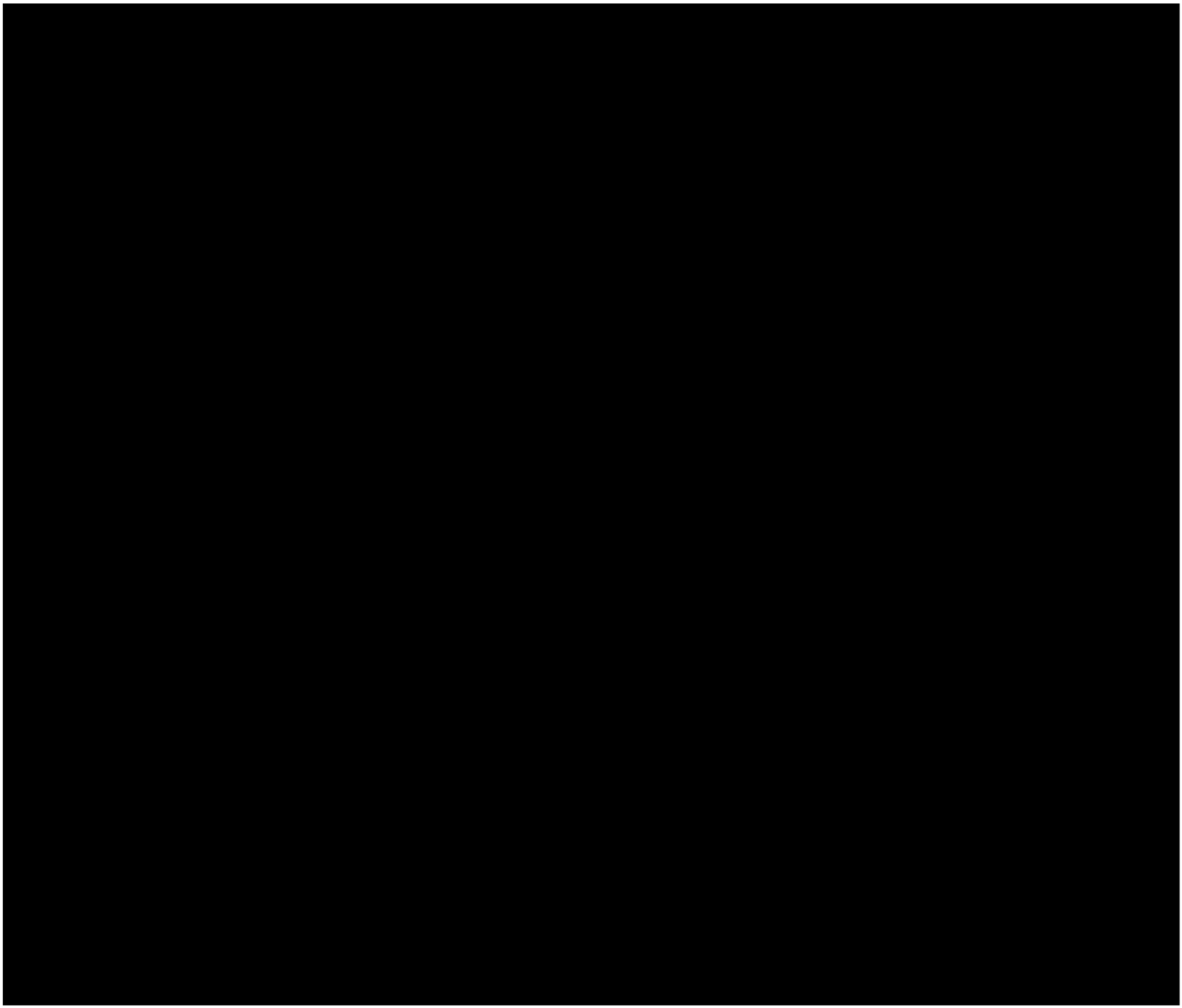
[redacted]

[redacted]

[redacted]



[redacted]



[redacted]

Introduction to Intelligence & the Intelligence Cycle

Information vs. Intelligence

The police gather information which is required for a policing purpose. Policing purposes 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 statute law.

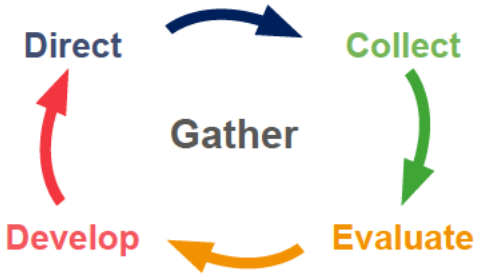
These policing purposes provide the legal basis for collecting, recording, evaluating, sharing and retaining police information. The recording of information is a professional requirement of the police service.

Police information undergoes an evaluation process which is appropriate to the policing purpose for which it was collected and recorded. All police information is evaluated to determine:

- Provenance
- Accuracy
- Continuing relevance to a policing purpose
- What action, if any, should be taken.

Evaluation involves searching and making connections with other records. This may require staff to search the different business areas and apply relevant evaluation criteria.

Therefore intelligence is information that has been reviewed, evaluated and graded accordingly, before being developed and disseminated. Information follows the Intelligence Cycle and is demonstrated below: -



Why submit Intelligence?

- To transfer intelligence from your own personal memory to the 'organisational memory' of the police.
- Allows the intelligence to be evaluated and actioned.
- Ensures the intelligence is held in accordance with the law.
- Ensures the intelligence can be shared and effectively linked, to provide an improved intelligence picture.

Intelligence Provides: -

- Foundation for warrant applications.
- Used on RIPA authorities.
- Grounds to search.
- Assists partner agencies.
- Identifies risk areas.
- Evidences the need for additional resourcing through the tasking process.

Intelligence Provenance

What is Provenance?

Provenance is the history or origin of something, and in the context of intelligence, it refers to the origin of the information, how and when it was discovered. There are three 'provenance' questions that need to be considered when collating intelligence. These are as follows:-

- How does the source know this?
- When did the source know this?
- Who else knows this?

It is only by answering these questions that the information can then be accurately graded and risk assessed accordingly. The provenance is therefore vitally important for all information but especially critical when considering threat, risk and harm, as well as firearms information.

Guidance on 3x5x2 & 5x5x5

The 5x5x5 grading system

Source Evaluation	**A** – Always Reliable	**B** – Mostly Reliable	**C** – Sometimes Reliable	**D** – Unreliable	**E** – Untested
Intelligence Evaluation	**1** – Known to be true without reservation	**2** – Known Personally to source but not to person reporting	**3** – Not known personally to source but corroborated	**4** – Cannot be judged	**5** – Suspected to be False
Handling Code	**1** – To UK police service & other law enforcement agencies	**2** – To Non-Prosecuting Parties in UK	**3** – To Non-EEA Law Enforcement Agencies	**4** – Within Gloucestershire Police only	**5** – No Dissemination refer to originator

The 3x5x2 grading system

Source Evaluation	**1** – Reliable	**2** – Untested	**3** – Unreliable		
Intelligence Evaluation	**A** – **Known directly**	**B** – **Known indirectly but corroborated**	**C** – **Known indirectly**	**D** – Not **Known**	**E** – Suspected to be False
Handling Code	**P** – Lawful sharing permitted	**C** – Lawful sharing permitted with conditions			

Comparison tables for the conversion of 5x5x5 into 3x5x2 intelligence reports

Source Evaluation

Old 5x5x5	New 3x5x2
A – Always Reliable B – Mostly Reliable	1 – Reliable
C – Sometimes Reliable D – Unreliable	3 – Not Reliable
E – Untested	2 – Untested

Intelligence Evaluation

Old 5x5x5	New 3x5x2
1 – Known to be true without reservation 2 – Known Personally to source but not to person reporting	A – Known directly
3 – Not known personally to source but corroborated	B – Known indirectly but corroborated
4 – Cannot be judged	C – Known indirectly D – Not known
5 – Suspected to be False	E – Suspected to be false

Handling Code

Old 5x5x5	New 3x5x2
1 – To UK police service & other law enforcement agencies 2 – To Non-Prosecuting Parties in UK 3 – To Non-EEA Law Enforcement Agencies	P – Lawful sharing permitted
4 – Within Gloucestershire Police only 5 – No Dissemination refer to originator	C – Lawful Sharing permitted with conditions

3x5x2 Explained

Source Evaluation

Source evaluation	1. Reliable	2. Untested	3. Not reliable

The source evaluation is made by the person submitting the information to describe the reliability of the source. This enables the credibility of the information to be established and informs the proportionality of tactical options.

Everyone submitting intelligence has a duty to ensure it is accurate and is corroborated where possible.

There are three source grading's:-

1). **Reliable** – This grading is used when the source is believed to be both competent and information received is generally reliable. This may include information from human intelligence, technical, scientific and forensic sources. It is important that the two tests of competence and veracity of past intelligence are both met before a source is considered to be reliable. Where either test is not met, **not reliable** should be selected and the grounds to doubt the reliability should be specified.

2). **Untested** – This relates to a source that has not previously provided information to the person receiving it or has provided information that has not been substantiated. The source may not necessarily be unreliable, but the information provided should be treated with caution. Before acting on this information, corroboration should be considered. This would apply to information when the source cannot be determined, for example, Crimestopper intelligence.

3). **Not Reliable** – This should be used where there are reasonable grounds to doubt the reliability of the source. These should be specified and may include concerns regarding the authenticity, trustworthiness, competence or motive of the source or confidence in the technical equipment. Corroboration should be sought before acting on this information.

Information/Intelligence Assessment

Information/ Intelligence assessment	A. Known directly to the source	B. Known indirectly to the source but corroborated	C. Known indirectly to the source	D. Not known	E. Suspected to be false

This grading describes the reliability of the information based on how it became known to the source and from other available intelligence.

A: Known directly to the source – Refers to information obtained first-hand, e.g. through witnessing it. Care must be taken to differentiate between what a source witnessed themselves and what a source has been told or heard from a third party.

B: Known indirectly to the source but corroborated – Refers to information that the source has not witnessed themselves, but the reliability of the information can be verified by separate information that carries the information/intelligence of assessment of A. This corroboration could come from technical sources, other intelligence, investigations or enquiries. Care should be taken when ascertaining corroboration to ensure that the information that is presented as corroboration is independent and not from the same original source.

C: Known indirectly to the source – Applies to information that the source has been told by someone else. The source does not have first-hand knowledge of the information as they did not witness it themselves.

D: Not known – Applies where there is no means of assessing the information. This may include information from an anonymous source, or partners such as Crimestopper intelligence.

E: Suspected to be false – Regardless of how the source came upon this information, there is a reason to believe the information provided is false. If this is the case, the rationale for why it is believed to be false should be documented in the intelligence report risk assessment

Handling Codes and Conditions

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.

Lawful sharing permitted (P)

In order to share this intelligence there must be:

- A policing purpose
- Local protocols in place
- A legitimate need to receive it.

Lawful policing purpose is defined as to:

- Assist others to protect life or property
- Assist to preserve order
- Prevent the commission of offences
- Assist others to bring offenders to justice
- Linked to any duty or responsibility arising from common or statute law.

Lawful sharing includes other government departments, private and voluntary sectors.

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?

Dissemination to European Economic Area (EEA) law enforcement agencies is permitted without any additional risk assessment.

If there are concerns around how widely the intelligence may be disseminated, Code C applies. It may not be appropriate to disseminate all of the intelligence and the merits of redaction should be considered.

Lawful sharing permitted with conditions (C)

This code permits dissemination but requires the receiving agency to observe conditions as specified. Application of this code means the originator has applied specific handling instructions in respect of this information. A risk assessment may be required in respect of the intelligence concerned. An application for public interest immunity should be considered if the intelligence is subsequently used in court.

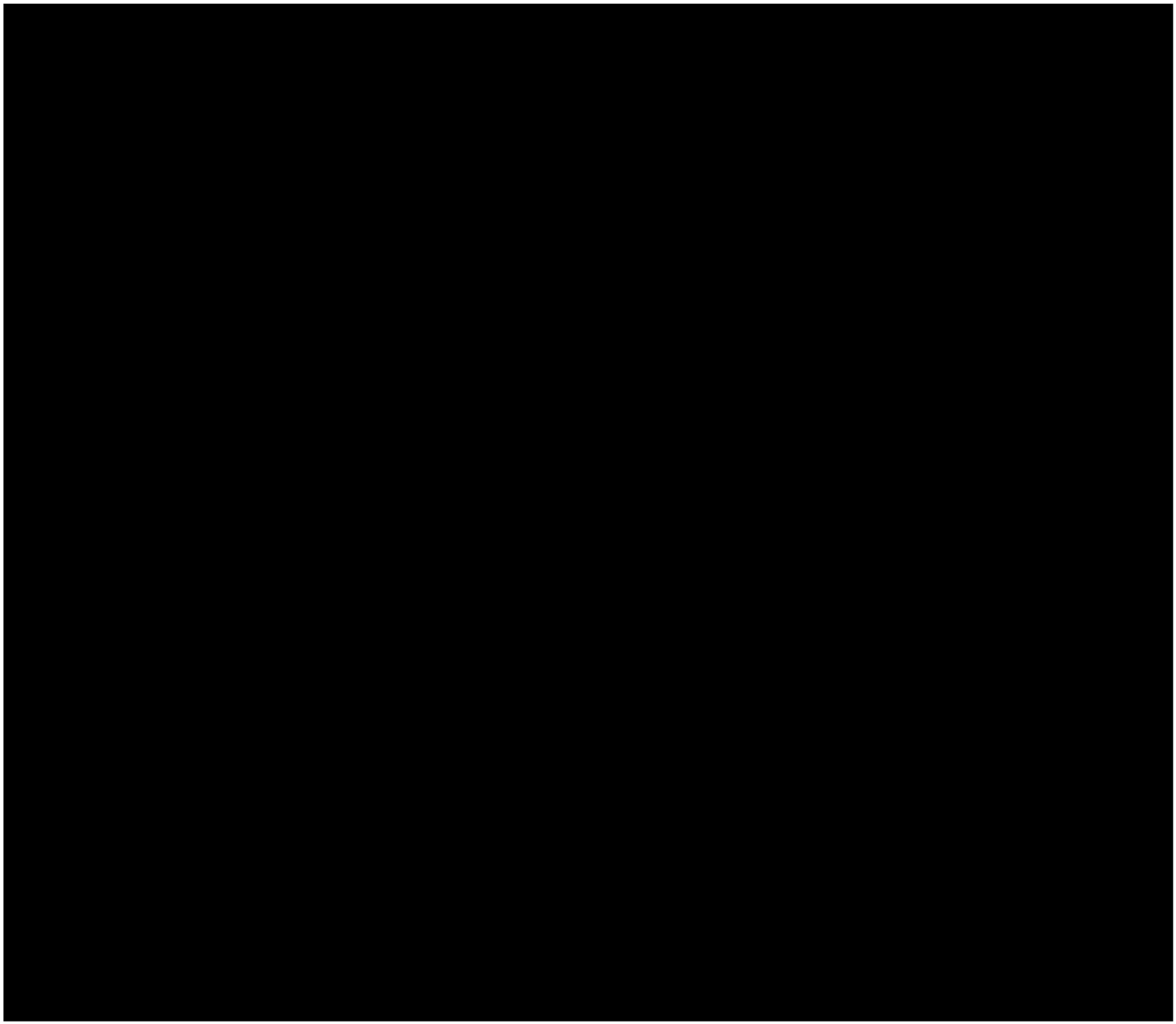
The recipient must abide by the handling conditions. The originator must be contacted by the recipient before they conduct any further activities outside the conditions.

Any intelligence report with conditions should remain under review to ensure that wider dissemination can occur as soon as is feasible, such as when an operation has been concluded or is no longer being pursued.

Conditions – Intelligence Unit only

- **A1 covert development** – intelligence may be combined or corroborated with other intelligence but action cannot be taken directly. Permission must be sought from the originator before action is taken on any derived intelligence.
- **A2 covert use** – covert action may be taken on this intelligence although the source, technique and any wider investigative effectiveness must be protected. This intelligence may not be used in isolation as evidence, in judicial proceedings or to support arrest.
- **A3 overt use** – overt action is permitted on this intelligence. This information can be used for: TO BE SPECIFIED BY SOURCE INTELLIGENCE OWNER.
- **S1 delegated authority** – the originator of the intelligence permits the unsupervised sanitisation of the material in order to allow dissemination to a wider audience.
- **S2 consult originator** – the originator of the intelligence does not permit the sanitisation of the material for wider dissemination without consultation being sought.

Government Security Classifications	Acquisition		Exploitation		
	Source	Intelligence	Handling	Intelligence Unit Only	
TOP SECRET	1 – Reliable	A –Known directly	P – Lawful sharing permitted	Action	Sanitisation
SECRET	2 – Untested	B – Known indirectly but corroborated	C – Lawful sharing permitted with conditions	A1 – Covert development	S1 – Delegated authority
OFFICIAL	3 – Not reliable	C – Known indirectly		A2 – Covert use	S2 – Consult originator
		D – Not known		A3 – Overt use	
		E – Suspected to be false			



[redacted]

Briefing & Tasking

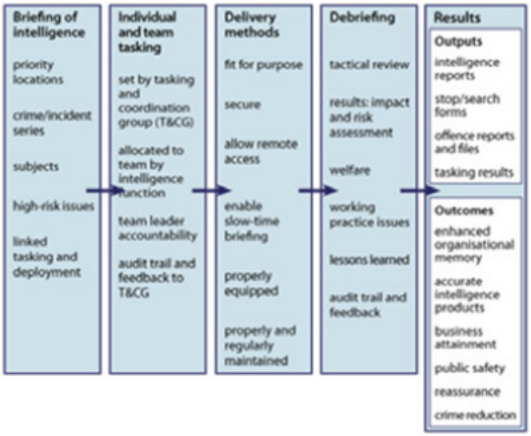
Intelligence briefing and related tasking are broad themes and a vital function for the Intelligence Department. Therefore, we need to consider 'Briefing' in the terms expressed in the National Intelligence Model, '*….an appropriately resilient briefing model [which] ensures the communication of intelligence that informs and directs operational policing activity….' This, rather than the more specific 'operational' briefing, defined by the Home Office as '..a meeting of relevant personnel before a deployment takes place…*'.

Furthermore, in terms of 'Tasking', we need to consider this in relation to the focus, allocation, recording and accountability of activity in response to the aforementioned briefing provision, rather than the Tactical Tasking and Coordination meetings, as defined within the NIM (which are discussed later in the guidance).

The National Briefing Model breaks down an effective process into five key elements.

- Briefing of Intelligence
- Individual and team tasking
- Delivery methods
- Debriefing
- Results

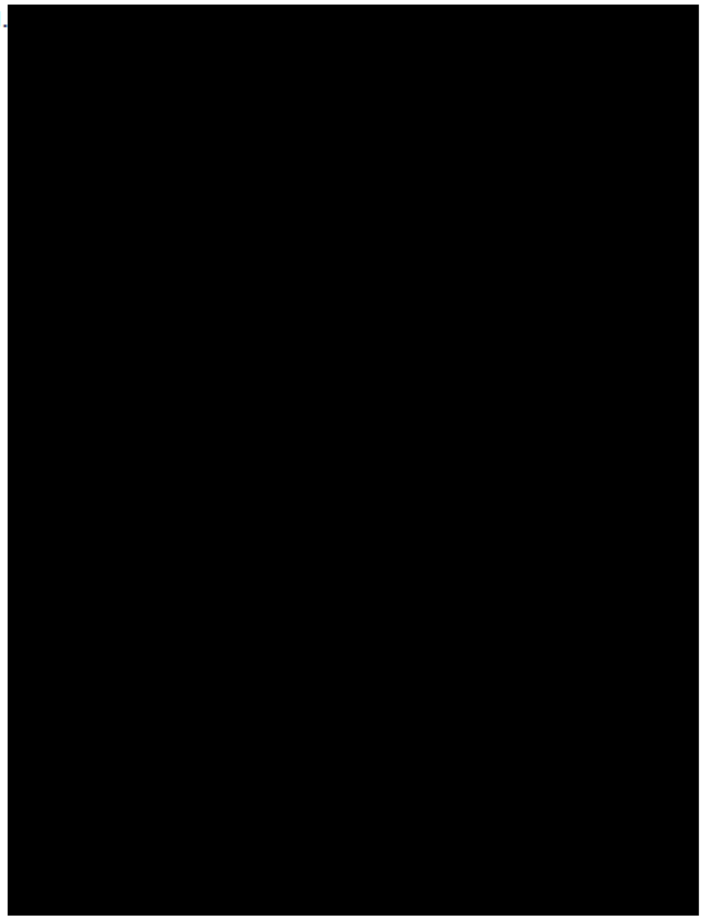
These can be further broken down, as follows…



Briefings should only be produced when assessed and prioritised and the content should be tailored to the needs of the team it is intended for. The number of briefings should be strictly limited to a figure that can be effectively appreciated and acted on by that team.

The system delivering this information needs to be secure and accessible to those who need it, and be relevant, contemporary, easy to use and aesthetically pleasing. The system should not only provide briefing bespoke to the audience, but have the ability to link efficiently with the allocation of activity, the management of the response and to record results in a visible and auditable way.

Should a member of staff require something to be published on briefings then the below template should be completed and sent into the FIB e-mail box, where this will be assessed and a decision made regarding the necessity of the briefing.



Gloucestershire Briefing Map

The NIM states that Chief Officers should, **'ensure that geographic crime and incident mapping technology is used to aid decision making, problem solving, communication and performance management…..'**

Work has been undertaken with ICT during the summer to configure and simplify the user interface of the ESRI mapping system. It has been used by some across the force but many are unaware of its usefulness or even existence. By benefiting from its daily interaction with the data warehouse, various layers of data can be populated and displayed on a detailed and scalable map, providing a 'self-briefing' tool for officers.

In addition to incidents, crimes and intelligence populating the map, there are now 'editable' layers for specific intelligence tasking and the organisation has scoped their use for mapping SARA plans and other local priorities.

All received intelligence does not, and cannot, result in a briefing slide. All (appropriate) intelligence will appear on the map however and activity can be carried out as a result. Some positive examples have already been noted following trials and these will increase as more users take advantage of this system. This is a work in progress but with incremental improvements, based on feedback from officers, this is a very beneficial tool which other forces visited do not have in this detail.

[redacted]

[redacted]

Intelligence Professionalisation Programme (IPP)

The reliance on using intelligence in the fight against crime is continually increasing. It is a Home Office requirement that all forces handle intelligence in the same manner in order to facilitate its exchange. This requirement followed cases where crimes were committed that could have been avoided had forces had access to each other's intelligence. To assist in the development of this the College of Policing has, with assistance from police forces across the UK, produced the Intelligence Professionalisation Programme (IPP).

The IPP covers all aspects of intelligence following from the first receipt of the information. It includes the methods used to record intelligence, any research or analysis carried out and the final dissemination. IPP is intended for those who are already in the field of intelligence. Decisions in respect of who should complete the programme are taken by the individual force.

All modules are to be delivered in force as follows:

- Introduction to Intelligence consists of a guide and some scenarios. The guide should be read by new entrants as soon as possible after joining, e.g. on the first day, as it provides a background to the discipline. The scenarios will be delivered by a trainer.
- Introduction to Research is classroom based and you must have completed the Introduction to Intelligence module or at least the guide before beginning this module.
- Introduction to Analysis is also classroom based and you must have previously completed the Introduction to Research module.
- Intelligence Manager consists of a guide and classroom based delivery of specialist subjects by experts in the field. Prior to this module you must have completed Introduction to Intelligence.

Introduction to intelligence

This module is intended for those new to the world of intelligence and provides an outline of the manner in which intelligence is treated. You should use the module as a reference or refresher throughout your career and also add to it as you become more experienced.

This module covers:

- The purposes for which Intelligence can be gathered
- Strategic and tactical intelligence
- The importance of intelligence

- The Intelligence Cycle
- National Intelligence Model
- The recording and dissemination of intelligence
- Disclosure
- Key roles in an investigation

Introduction to Research

This module is for all who carry out research, not just those who are Researchers within an intelligence unit, as it can be useful for officers and staff in other disciplines within law enforcement. It is classroom centred training, based on participation and is a prerequisite for anyone undergoing analyst training.

The module contains sections on the following:

- The role of the researcher
- Terms of reference
- Creative thinking techniques
- Mind sets and biases
- Collection for research and collection plans
- Evaluation
- Basic statistics
- Techniques for challenging
- Reports and briefings

Introduction to Analysis

This module is intended for analysts within intelligence and is made up of classroom based training.

The module includes the following:

- Creative thinking techniques
- Processes for evaluating intelligence

- The value of using visualisation techniques in order to identify intelligence gaps and to highlight key intelligence issues
- Development of a scenario using visualisation techniques
- Developing and testing hypotheses including how logic and perception can affect an analysis
- Challenge techniques including the value of critically evaluating inferences and judgements to improve the quality of analytical products
- How to structure and deliver written and oral briefings in order to deliver their analytic judgements/ inferences effectively

Role of an Analyst

Analysts are deployed in support of problem solving and to inform those making decisions through tasking and coordination processes. Analysis supports this by identifying and developing an understanding of problems to help decide which of these problems should be prioritised. They must also be able to:

- Discuss and develop terms of reference for an intelligence analysis product
- Obtain and evaluate information for intelligence analysis
- Apply analytical techniques to interpret information for intelligence analysis
- Use inference development to make judgements based on intelligence analysis methods
- Develop recommendations based on the results of the intelligence analysis methods
- Create an intelligence analysis product to support decision making
- Disseminate the intelligence analysis product
- Review the effectiveness of the intelligence analysis product.

Role of a Researcher

The researcher is responsible for:

- Searching and retrieving information
- Synthesising intelligence and other material
- Establishing facts
- Compiling reports and presenting their findings.

It is not always possible or necessary to employ an analyst and a researcher together. While an analyst is able to undertake their own research, a researcher cannot undertake analysis. In addition, an intelligence researcher must be able to:

- Obtain and evaluate information for intelligence analysis
- Disseminate the intelligence analysis product
- Research, prepare and supply information.

Analytical Techniques

Analytical techniques can be used to understand and predict threat, harm, risk and opportunities. A combination of these techniques can be used to identify prevention, reduction and disruption opportunities. Their practical application is outlined below.

Crime Pattern Analysis (CPA) identifies the nature and scale of emerging and current crime and disorder trends, linked crimes or incidents, hot spots of activity and common characteristics of offenders and offending behaviour.

Those undertaking analysis should have a general awareness of the types of crime and disorder within their geographical or specialist scope. This makes it easier to identify patterns as they emerge as well as any unusual or developing event factors.

There are four main types of CPA:

- Hot spot identification
- Crime and incident trend identification
- Crime and incident series identification
- General profile analysis.

Demographic and Social-trend Analysis (DSTA) examines how demographic and social changes within an area or within a demographic group can affect levels and types of crime and disorder.

These changes may be due to an individual incident such as a live music event, or may, for example, be because of a long-term change in either the ethnic make-up or age profile of a geographical area. DSTA is often used to develop an understanding of a particular problem which has been identified by crime pattern analysis.

Network Analysis provides an understanding of the nature and significance of the links between entities. It also assesses the strengths and weaknesses of criminal groups or organisations such as in Organised Crime Groups.

Network analysis:

- Provides a detailed picture of the roles played by individuals, including their rank in a hierarchy and level of control
- Supports the identification of intelligence gaps and subjects to target
- Gives an understanding of the scale and seriousness of the threat posed by criminal groups
- Shows associations within and outside the network
- Identifies key areas and possible tactics for investigation and disruption
- Focuses intelligence gathering
- Will often be developed using graphical software to demonstrate the links between people, objects, communications data, locations and events
- Can be used to examine the type of links between entities, including between people who are not believed to be committing criminal offences, for example, links between victims or family associations and relationships.

Market Analysis identifies the criminal market around a commodity or service, and can be used to describe a criminal market at any level. Market analysis is used to:

- Outline the level of activity of a market
- Identify emerging market trends
- Understand and explain how and why the market operates
- Assist the selection of subjects for targeting
- Highlight potential new sources of information.

Criminal Business Analysis (CBA) is used to develop an understanding of how criminal activity, businesses and techniques work. It is especially useful for technical, complicated and new criminal activity.

CBA is used to:

- Develop knowledge and understanding about the way criminals work
- Identify key points for disruption
- Provide information to focus intelligence gathering
- Predict criminal activity
- Facilitate investigative techniques
- Identify requirements for alterations in resource levels to meet unprecedented threats.

Risk Analysis is a technique that can be used to support threat assessment. It can be applied to a range of different situations in order to identify the likely impact of law enforcement action or inaction, and to predict criminal activity. Risk analysis supports the assessment of the scale of the risk posed by individual offenders, organisations or crime types to potential victims, the public generally, law enforcement agencies or the criminal justice system. Gloucestershire Constabulary uses the Management of Risk in Law Enforcement (MoRiLE) for threat assessment.

Results Analysis evaluates the effectiveness of an activity. This could include:

- Enforcement tactics
- Intelligence gathering
- Impact of activity
- Cost benefit analysis
- Cause and effect analysis.

It also includes whether the crime or incident levels have changed in the way expected as a result of the operation or initiative.

Results Analysis:

- Identifies effective practice and highlights areas for improvement
- Recommends the discontinuance of ineffective strategies
- Ensures investment in what works
- Facilitates knowledge management

- Provides valuable input to the knowledge products and organisational memory database
- Supports resource decisions
- Aids the development of skills and knowledge levels of personnel
- Monitors the progress of plans
- Assesses the effectiveness of pilot projects
- Aids and refines professional development
- Identifies unintended consequences

The National Intelligence Model

The National Intelligence Model (NIM) is an intelligence based deployment system. The NIM identifies crimes patterns and intelligence, through a variety of sources, to allow focused deployment of limited resources through the Tactical Tasking & Co-ordination Group (TT&CG).

The information for the TT&CG is gathered by utilising the following assets: -

Knowledge Assets

- Briefing products
- Current Legislation
- Codes of Practice
- Force policies and procedures
- THRIVE+ model
- National Decision Model
- Code of Ethics

System Assets

- Investigatory Powers Act 2016
- Information Sharing Protocols
- Analytical tools (Management of Risk in Law Enforcement - MoRiLE)
- Organised crime group mapping (OCGM)
- Police National Database (PND)
- Crime recording systems
- STORM
- Violent Offender and Sex Offender Register (VISOR)
- National Ballistics Intelligence Service (NABIS)

Source Assets

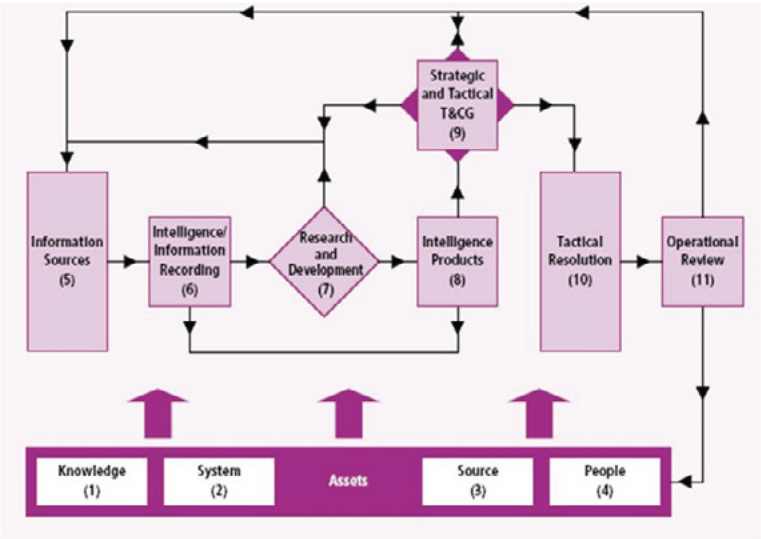
- Victims & Witnesses
- Communities

- Crime Stopper intelligence
- Prisoner Debriefs
- Forensic information
- Surveillance product
- Covert Human Intelligence Sources (CHIS)

People Assets

- TTCG Chair and attendees
- Director of Intelligence
- Central Authorities Bureau
- Telecoms SPOC
- Intelligence Manager / Supervisor
- Analysts & Researchers
- Intelligence Officers
- Local Policing
- Specialist Crime

National Intelligence Model (NIM)



Tasking & Co-ordinating

The tasking and co-ordination process provides managers with a mechanism for operational decision making at strategic and tactical levels. Proactive leadership is essential in this process. To enable managers to prioritise the deployment of resources, decisions should be based on a thorough understanding of the problems. Forces should have a system for recording all tasking and co-ordination decisions, operational plans and results.

Strategic Tasking & Coordinating

Strategic tasking and coordinating is part of police governance and planning. The strategic tasking and coordinating process enables senior managers, through a strategic tasking and coordination group (ST&CG), to consider and agree strategic direction and align resources to force priorities.

The purpose of the ST&CG is to:

- Consider the operational priorities recommended in the strategic assessment
- Set and amend the control strategy, where necessary
- Approve a strategic intelligence requirement
- Consider prioritisation of resources.

Tactical Tasking & Coordinating

Tactical tasking and coordinating is part of the police response to operational priorities. The process enables senior managers, through a tactical tasking and coordination group (TT&CG), to consider and agree tactical options and align resources to priorities.

All decisions made by the TT&CG must be recorded to provide an audit trail and ensure accountability. It is good practice to have an action manager who, with the authority of the TT&CG chair, oversees progress against delivery plans. Results analysis should be used, where appropriate, to measure the impact and success of delivery plans.

The TT&CG should:

- Consider the tactical assessment and create operational delivery plans
- Apply the control strategy
- Ensure that decisions about priorities and resources are based on the best available threat assessments (MoRiLE scores)

- Manage competing demands
- Establish a rational basis for decision making
- Review intelligence requirements
- Commission further development of analysis to find out more about issues described in the tactical assessment
- Decide on prevention, intelligence, enforcement and reassurance actions
- Allocate resources and assign plan owners
- Consider tactical recommendations from the intelligence unit meeting
- Consider escalation where an issue is beyond the capability of the resources available to the T&CG
- Commission operational review
- Review whether plans and intervention work are still meeting objectives.

FIB Monthly Threat Assessment

The newly formed FIB Monthly Threat Assessment Meeting (September 2018) is a monthly review of the current Gloucestershire Threat Assessment and Intelligence Summary, including the management of any potential actions. The objectives of the meeting are as follows: -

- Prioritise the identified threats and operations that will be subject to active intelligence development prior to Force TT&CG.
- Allocate and manage actions.

The meeting is chaired by the Director of Intelligence and the attendees include the various areas of business in the Intelligence Directorate.

[redacted]

Intelligence Collection Plans

Intelligence Collection Plans help to close gaps in knowledge. They focus on **Intelligence Requirements** and provide a structure for the collection of information. Intelligence requirements outline the information required or questions that need answers, in order to fill gaps in an investigation or operation. The content of an intelligence collection plan varies according to the intelligence that is required.

Intelligence may be collected from a variety of data sources, including:

- Community Intelligence
- Forensic intelligence product
- Communications Data
- Covert Human Intelligence source (CHIS)
- Prisoner De-briefs
- Tasking through briefing products.

Intelligence Collection Plans should:

- Be updated regularly so that information collection can be properly managed, ensuring gaps, additional potential sources and possible access difficulties are identified.
- Contain the necessary information requirements in order to inform a comprehensive and accurate intelligence picture.
- Justify the proportionality and necessity of the activities that will be used for collecting the information.

Subject Profiles

These are usually commissioned by the tactical tasking and coordination group to provide a detailed report of a suspect(s) or victim(s). Each profile has an assigned owner and is added to and updated until the subject is apprehended or protected. Subject profiles may also be commissioned by a senior investigating officer to assist investigations during a major or serious crime inquiry including firearms operations as well Kidnap & Extortion investigations or an intelligence manager to aid research.

A subject profile is created to:

- Assist in prioritisation
- Identify intelligence gaps
- Highlight prevention, intelligence, enforcement and reassurance opportunities
- Provide justification for actions.

Justification for the selection of subjects and the tactics deployed must comply with the principles contained in the Human Rights Act 1998. Subject profiles should be stored centrally to enable information to be retrieved if necessary.

Content of the subject profile

The subject profile should be based on the research and analysis of a wide range of information sources (closed/open), including OCGM and external information. They should include a risk assessment which identifies the effect of a range of impact factors and suggests actions to counter or minimise them. They should have the appropriate GSC marking, and comprise of the following categories.

Summary and authorisation:

[redacted]

Personal record:

[redacted]

[redacted]

[redacted]

Subject Profile Analysis:

[redacted]

Search Warrant Applications

Before any search warrant application is made an officer receiving the information is responsible for reviewing it and considering its accuracy, how recent it is and accessing the grading. If the intelligence is anonymous, corroboration should be sought. If there is additional intelligence that may undermine the application this should also be listed on the application in order that the full facts can be considered. Discuss the application with FIB supervisors to ensure that the application does not impact upon ongoing operations.

There are 2 main powers which a search warrant can be applied under -

1) Section 8 of the Police and Criminal Evidence Act 1984

A Justice of the peace may issue a warrant if they are satisfied by information on oath that there is reasonable grounds for believing -

That an indictable offence has been committed; and that there is material on premises which is likely to be of substantial value to the investigation of the offence; and that the material is likely to be relevant evidence

If applying for a S8 warrant you must indicate what offence you are investigating not the search power you are using.

2) Section 15/16 of the Police and Criminal Evidence Act 1984

This allows the issue to constables under any enactment of warrants to enter and search premises.

A common example of this is S23 Misuse of Drugs Act. Other search powers include section 26 of the Theft Act 1968, section 46 of the Firearms Act 1968 and paragraph 1 of Schedule 5 to the Terrorism Act 2000.

A Justice of the peace may issue a warrant if they are satisfied by information on oath that there is reasonable grounds for suspecting - For e.g. in the case of S23 MDA controlled drugs are in the possession of a person on any premises; or that a document directly or indirectly relating to a transaction or dealing which is in the possession of a person on any premises.

The Magistrates may ask why you are applying under section 8 and not through S15/16. Remember a warrant under S23 MDA requires suspicion that drugs are within the premises whereas under S8 PACE you need to believe that an indictable offence has been committed and believe that substantial evidence is held within that premises. Belief is a higher threshold than suspect.

Applications for a warrant shall be made ex parte and supported by written information. The constable shall answer on oath any question that the justice of the peace or judge hearing the application asks them. Good information should anticipate questions likely to be raised by the Magistrate and should form part of

the officer's research. S107 PACE states that an Officer performing a duty at a higher rank i.e. an Acting Inspector will have the same level of authority as a substantive Inspector and therefore is able to authorise a warrant application. The accuracy of the information is paramount and if found to be flawed during the hearing the application is likely to be refused.

To find the current forms for the search warrants and the information visit the intranet.

Please note that there are extensive notes for guidance on the forms themselves and this brief guide should be read in conjunction with the notes on the warrant application form.

The information should broadly contain the following;

Correct legislation and provision

What the test is (suspect or belief)

How the test is satisfied

The intelligence case

Analysis of the strength of the application

Previous similar convictions

Grading of the intelligence (Reliability)

Amount of intelligence

Time period / currency of the intelligence

Corroboration of intelligence

Anything that mitigates against the application

Consider proportionality, why do you need a warrant? Would a lesser measure suffice?

Sensitive Intelligence

Consider anything used to obtain a warrant is potentially disclosable to the defence. This includes information given verbally under oath as the Magistrate and applicant have an obligation to produce a record of all information provided to obtain the warrant.

Consider:

Do I need to rely on sensitive intelligence to succeed?

Can I reveal the sensitive intelligence to the court?

Contact Gloucestershire FIB or SIU to discuss the use of sensitive intelligence.

Articles Sought

It is important that you describe the items that you are searching for to the Magistrates and this should be documented on the application and the search warrant. It is unlikely that Magistrates will authorise generic warrants which may be viewed as a 'fishing trip'. Try and be specific for e.g.

[redacted]

The premises

What links your information to the address? You should corroborate the intelligence using other Police systems, Benefits Agency, housing, name/address checker etc.

All premises warrant- there is a power to obtain this type of warrant if deemed suitable. The warrant would be issued giving the police the power to search all premises connected to the subject. There is an obligation to list all known addresses on the schedule and then state why it is not reasonably practicable to specify all other premises

If applying for this type of warrant, special care is required. Case Law (R v Bhatti and R v Redknapp) has decreed that the copy of the warrant provided to the occupier must include a copy of the schedule otherwise the Officers have not complied with section 15 of PACE, resulting in the execution of the warrant being unlawful and the return of seized items. If for operational reasons you do not want to disclose the other known addresses on the schedule to the subject, then consideration needs to be made to apply for separate warrants or the details of other addresses can be redacted from the schedule.

Other persons accompanying the police need to be listed on the warrant. E.g. - SOCO officers, other agencies such as trading standards etc.

Documents required upon attendance at Court;

The information (1 copy) and written search warrant forms (3 copies)

Any documents that materially assist the application

Any documents that detract from the application. In addition if suitable marked maps, plans and photographs of areas to be searched.

The Court Application

S15 (4) PACE - The Constable shall answer on oath any questions that the Justice of the Peace or Judge hearing the application asks of them.

Anticipate questions and include these in the written information.

Know the content of your information and be prepared to answer questions. If you are unable to answer the questions posed by the Magistrate, you are unlikely to get your warrant authorised.

Make a note of any questions asked and your answers. This forms part of your application and will protect against unwarranted allegations and allow the reviewing court to know the basis of the application (R v Cronin).

Execution of the search warrant

The warrant must be executed within the time frame stated. 28 days for a MDA warrant and 3 calendar months for a S8 warrant.

If there is a significant delay from obtaining to actioning the warrant then a review needs to be completed as to whether there has been a material change in the basis on which the warrant was granted.

[redacted]

A copy of the warrant must be provided to the occupant of the premises or left at the premises if nobody is present. Details of property seized must also be provided to the occupant.

A search warrant should be returned to the Magistrates court when it has either been executed or when it has expired. The court will retain the warrant for an additional 12 months, during which it is available for inspection by the occupier of the premises to which it relates.

Out of hours warrants

The new scheme came into force at 6am on 1 September 2018. [redacted]

For use of urgent applications, see criteria below;

- There is danger to life, limb or health of an individual
- An offence will be committed if urgent action is not taken
- Property / evidence will be lost if no action is taken and there is no other authority available.

In this context immediate action means that the warrant must be executed before the court reopens at 10 a.m. on the next working day. In determining whether to allow an application to be made the legal adviser will have regard to how long the information has been in the possession of the applicant.

Covert Human Intelligence Source (CHIS)

A CHIS represents a potentially useful source of information and a valuable asset for law enforcement. Therefore all staff must have a basic understanding of how, and under what circumstances, a person becomes a CHIS.

The legal definition of a CHIS is provided by the Regulation of Investigatory Powers Act (RIPA) 2000.

Section 26(8) of RIPA classifies a person as a CHIS if:

a) he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph (b) or (c);

b) he covertly uses such a relationship to obtain information or to provide access to any information to another person; or

c) he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

Section 26(9) of RIPA defines a covert relationship as follows:

d) a relationship is used covertly, and information obtained as mentioned in subsection (8)(c) is disclosed covertly, if and only if it is used or, as the case may be, disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.

It is the action of the individual, on behalf of the law enforcement agency and in the manner described, that constitutes their status as a source that requires authorisation. Merely providing information to a law enforcement agency that is already within the individual's possession does not necessitate authorisation.

Status Drift

Individuals or organisations that, because of their work or role (travel agents, housing associations, taxi companies) have access to personal information may provide information to the police on a repeated basis. They, therefore, need to be managed appropriately.

Information provided by individuals or organisations on a repeated basis are referred to as frequent contacts. A review by the intelligence unit must take place after an individual or organisation has had a maximum of three repeated contacts with the police.

The purpose of the review is to determine whether an individual or organisation:

- Is being managed with an appropriate level of sensitivity and confidentiality;
- Should be considered for registration as a CHIS.

There is no specific time period to becoming a frequent contact. Determining the status of an individual or organisation is a matter of judgement by the intelligence unit and will be considered in consultation with the reporting member of staff. Therefore, this process identifies **status drift**, which identifies the status of the person reporting information to the police. The drift element is concerned with a member of the public reporting information to the police, to them being identified as a person having a covert relationship, in order to obtain the information, meaning their status could drift into that of a CHIS.

Individuals who are deemed suitable for registration as a CHIS will be referred to the Dedicated Source Handling Unit (DSHU). It is important that all staff are aware of these issues concerning frequent contact, as this will avoid any potential implications of status drift; as there is also personal responsibility for identifying these drift issues, as well as that of the intelligence unit.

Sensitive Intelligence

Sensitive Intelligence is information that has been reviewed and evaluated in the normal manner, as like any other piece of information. However, if during the evaluation process it is identified that there are concerns regarding the some of the following (not an exhaustive list), then there is a requirement to complete a risk assessment, and classify the information as sensitive: -

- the identity of the source
- the limited number of people having knowledge of the information
- any identified risks to the source from having passed the information onto the police
- the manner in which the information was gathered (i.e. covert techniques used)

This means that if using the 5x5x5 intelligence grading system, the intelligence would either have a handling code of 4 or 5. Whereas under the new 3x5x2 grading system the intelligence would have a handling code of (C) – Lawful sharing permitted with conditions.

Risk Assessments

Any information marked with the above handling codes, whether it is the 5x5x5 system or the new 3x5x2 grading system, requires special attention. The application of these codes means that the originator has applied specific handling instructions in respect of the information. It is possible a risk assessment will be required in respect of the information concerned and that if it is subsequently used in court, an application for Public Interest Immunity (PII) will be sought. If there are concerns regarding the source of the information or a risk to others is identified through the evaluation process, then a risk assessment must be completed.

The risk assessment process also includes consideration of ethical, personal and operational risks in respect of the source, the information content, its use, dissemination and compliance with a legislative requirement or policing purpose. This process also includes a justification for the decisions made and appropriate details of appropriate authorisation. It considers the proportionality, accountability, and necessity for recording, disseminating and retaining the information. The risk assessment considers the following information:

- **Confidential Material** – is the information confidential material?
- **Special Handling Conditions** – does further dissemination require the prior approval of an FIB Supervisor?
- **Risks** – could improper disclosure result in a serious risk of harm to the source of the information?
- **Dissemination Purpose** – is this to manage further tasks, develop the intelligence within the confines of

the handling conditions, or minimise the risks?

- **Special Conditions** – if disclosure is required then does there need to be a PII application?
- **Risk Management Plan** – this may be to protect the source of the information for future disclosure or if disclosure is required then there needs to be PII considerations or non-disclosure if there is too much risk to the source.

Public Interest Immunity (PII)

Public Interest Immunity (PII) is the legal principle that enables the courts to reconcile the two conflicting public interests, these being:

- The public interest in protecting the identity of covert human intelligence sources or covert methods from disclosure.
- The public interest in the fair administration of justice.

Where this conflict arises, and unless a decision is taken to abandon the prosecution, it is necessary to seek a ruling from the court as to where the overall balance of the public interest lies. This involves emphasising to the court that the material the law enforcement agency wishes to withhold is subject to public interest immunity and should not be disclosed.

The principle of PII is an exception to the general rule that relevant material will always be disclosed. It does mean, however, that special care needs to be taken in deciding where the balance lies between the two competing public interests before a decision as to disclosure is made.

Examples of material which is likely to attract PII (not an exhaustive list):

- Material that contains matters of national security
- Material which discloses the identity of members of the Security Service
- Material which would disclose the existence and/or identity of a CHIS
- Material which would disclose the true identity of an undercover operative
- Material which, if it were to become known, might facilitate the commission of other offences
- Material which, if it were to become known, would alert someone not in custody that they were a suspect
- Material which would disclose covert surveillance methods, the locations used or other sensitive methods of detecting crime

- Information received by (and/or assistance provided to) an investigator on a confidential basis
- Reports submitted by the investigator to the prosecutor
- Material referring to child witnesses
- Material upon which search warrant applications are made

Threat to Life (TTL)

The case law surrounding the case of Osman v UK, confirmed the positive obligation on the police under Article 2, European Commission of Human Rights (ECHR) to take reasonable steps to protect potential victims from a real and immediate threat to their lives, which is attributable to the actual or threatened criminal acts of a third party. It applies where the following criteria are met:

- Deliberate intention or criminal act of another
- Real & immediate threat identified (by Police or other law enforcement)
- Result would be death, serious harm or injury (to another) including serious sexual assault & rape

The definition of 'real & immediate' danger should be taken literally, where a reasonable/objective assessment of the threat suggests it to be genuine and the offender has both the intent and capability to carry it out. It is not necessary to show that the threat will materialise in the very near future; if the capability of the person making the threat is dependent on them finding a suitable opportunity to carry it out, the threat can still be deemed 'immediate' in that it is 'present and continuing' and may persist for some time.

The distinction between a TTL and a 'Threat to Kill' will depend on the nature of the threat, how it was received and from who/what. Generally a 'Threat to Kill' is an overt/explicit threat amounting to a substantive criminal offence and can be dealt with accordingly. A TTL will usually arise from sensitive intelligence, requiring a covert response and can be extremely challenging to prove evidentially.

The main objectives of the TTL policy are:

- Protect the life of any intended victim(s)
- Preserve the lives of all others involved
- Prevent serious injury
- Ensure public safety
- Maintain the safety of all those involved in attempting to mitigate the risks

- Protect intelligence sources
- Provide a standardised national framework for dealing with such incidents with other agencies and across force boundaries

Initial Action

A Threat to Life may be received in a number of ways, but it will inevitably fall into one of two categories. It will be either:

- A threat identified by the police or other law enforcement agency during an investigative process.
- A threat coming to police or other law enforcement agency's attention from an intelligence source(s).

Therefore a TTL will follow a logical path, although the urgency of any given situation will sometimes compress the separate stages of the process. Initially the assessment and the responsibility for ensuring any immediate action is taken to preserve life, is that of an Inspecting rank. However, any member of staff receiving a TTL is responsible for obtaining all information and notifying the Duty Inspecting Rank immediately. The sequences of events are:

- Identification or receipt of the threat.
- Documented Assessment of the nature and severity of the threat (to include an initial investigation and classification).
- Response to mitigate the threat/risk – i.e. devising and initiating a strategy for preventative or disruptive measures.
- Resolution – initiating the agreed strategy leading to the removal of the threat/risk.
- Monitoring – maintaining an overview of risk management measures and managing the level of risk as dictated by the developing intelligence picture.

The threat assessment establishes the level of risk, these being Low, Medium or High. Dependent on the risk level, is dependent on the way the TTL is dealt with.

Low Risk (managed by Inspector rank)

[redacted]

Actions regarding 'Low Risk' - The assessment conclusion will be recorded on the STORM log if appropriate and should make reference to the intelligence unless directed otherwise by a Superintendent rank. The conclusion that a threat is 'Low' does not eliminate the need for an investigation of it to ensure its origin or potential for escalation is understood (e.g. one of a series of reports made). Where a crime has been recorded the assessment conclusion will be recorded on the updated crime report and the usual processes of recording and investigating such incidents should also continue.

Where an intelligence entry is made it must include permissible identifying details of both suspect and intended victim where possible, and an indication of the nature of the threat, result and the date. The fact that an assessment has been carried out is also to be included.

If any additional information comes to light at a later stage that indicates that the threat has been increased, an Inspecting rank will be responsible for ensuring that the matter is reassessed and any necessary action taken.

Medium Risk (managed by Superintendent rank)

[redacted]

[redacted]

Actions regarding 'Medium Risk' – Where the threat is assessed as being greater than 'Low', a Superintendent must be informed and will be responsible for reviewing all the information concerning the threat/risk and for making an assessment of it. Where this confirms that the risk is 'Medium', an Investigating Officer (IO) must be appointed to assume the responsibility to manage the delivery of the police response. In appropriate cases the option to declare this as a 'Critical Incident' must be considered.

[redacted]

The Superintendent must ensure that an appropriate record of events and facts is maintained in a version

of the Threat and Risk Assessment tracking document supported by Force intelligence system entries. If the Superintendent decides that no entry should be made on the system they must record that decision and the rationale for it.

High Risk (manage by Superintendent rank)

[redacted]

Actions regarding 'High Risk' – Where the threat is assessed as 'High', the Superintendent will be responsible for taking all immediate action to minimise the threat to the intended victim, the public and the law enforcement officers and must declare this as a 'Critical Incident'.

The Superintendent must ensure that an appropriate record of events and facts is maintained in a version of the Threat and Risk Assessment tracking document supported by Force intelligence system entries. If the Superintendent decides that no entry should be made on the system they must record that decision and the rationale for it.

[redacted]

[redacted]

Investigatory Powers Act (IPA) 2016

The Investigatory Powers Act (IPA) governs how we use the investigatory powers available to us.

These powers include:

- Targeted Interception
- Equipment Interference,
- Communications Data
- Bulk equipment interference and intercept.

The IPA brings together all of the powers already available to law enforcement and the security and intelligence agencies, to obtain communications and data about communications. It overhauls the way these powers are authorised and overseen, introducing a 'double-lock' for interception warrants, so that once authorised these warrants cannot come into force until they have been approved by a judge. The IPA creates a powerful new Investigatory Powers Commissioner (IPC) to oversee how these powers are used.

The IPA affects the way we conduct investigations and impacts key law enforcement roles.

These include:

- Introduces a number of new offences. If you are using these powers you must ensure you know what these offences are so that you can avoid acting unlawfully.
- Changes the way we use related powers in other legislation. If you use the wrong legislation the activity will not be authorised and the operation will be impacted.
- Introduces opportunities to improve decision-making and streamline processes, however, it also introduces a new, more robust oversight regime, which means that there will be more external scrutiny of the use of these powers.
- Creates new, enhanced safeguards for private information and particular groups such as MPs and journalists. This includes new obligations for applying for and the safe handling, storage and destruction of information.

For law enforcement purposes the main areas of focus are the powers for the following capabilities:

Communications Data - i.e. information about communications: the 'who', 'where', 'when', 'how', and 'with whom' of a communication but not the content (i.e. what was written or said).

Targeted Equipment Interference - This enables interference with electronic equipment for the purposes of obtaining information or communication but not interception. This is a new provision for law enforcement,

although law enforcement agencies are already able to authorise Targeted Equipment Interference under other legislation.

Targeted Interception - Previously referred to as Lawful Intercept - this is the process of legally making the content of a communication available to law enforcement and/or other agencies. These powers are not widely available to LEAs.

The IPA is not a 'like for like' replacement for existing legislation - many aspects of those Acts remain in place. It does, however, change the way you use those powers.

Regulation of Investigatory Powers Act (RIPA) - RIPA provides powers for the use of Covert Human Intelligence Sources and Directed and Intrusive Surveillance. These have not changed and are likely to be used with the IPA powers.

The IPA, however:

- Replaces the RIPA powers for Communications Data and Lawful Intercept. The IPA should, therefore, be your first point of reference for use of these powers.
- Enables you to combine surveillance activity within a Targeted Equipment Interference warrant if the activity is to for that purpose i.e. a separate Directed or Intrusive surveillance authority under RIPA is not needed.

Police Act 1997 - The IPA introduces a restriction on the use of Property Interference powers within the Police Act. In simple terms, you cannot use these powers if your intention is to interfere with electronic equipment for obtaining information (you should use the IPA Targeted Equipment Interference powers instead).

The IPA introduces the powerful new role of the Investigatory Powers Commissioner (Lord Justice Fulford) who is heading up the new oversight regime, which will be delivered through the Investigatory Powers Commissioner's Office (IPCO). IPCO also oversees the use of investigatory powers in RIPA and the Police Act. IPCO's role covers:

- Authorising and approving the use of investigatory powers. This is done by Judicial Commissioners sitting within IPCO (serving or former High Court Judges). You may hear this referred to as the 'double lock'.
- Inspecting public authorities on their use of the powers. This is done by a number of expert inspectors.
- Informing Parliament and the public about the need for and use of powers. This is mainly the responsibility of the Investigatory Powers Commissioner.

Covert Authorities Bureau (CAB)

The Covert Authorities Bureau (CAB) deal with telecommunication providers - phone and internet networks such as EE, Vodaphone and Sky, in order to progress enquiries regarding phone attribution and communications data. This also includes IP addresses, email addresses and similar information. In addition, they are the gatekeepers for all covert policing. They will answer questions on issues such as the lawfulness and the level of authority required to install a memo cam in an address, or how many times you can check Facebook before it becomes surveillance. Furthermore, the CAB will also now manage applications under the new Investigatory Powers Act (IPA) 2016.

Digital Intelligence Unit

The Digital Intelligence Unit holds our expert Digital Media Investigator's (DMI's) and experienced Open Source Intelligence (OSINT) researchers.

The DMI's can provide a digital strategy for an enquiry, advise on and support specialist digital tactics and suggest which route is most appropriate; linking traditional policing, the Digital Forensic Unit (DFU) and the Central Authorities Bureau (CAB).

The OSINT researchers can help with mid to high level research for enquiries and can evidentially capture Facebook pages and similar. Guidance will also be given as to when Directed Surveillance Authorities are needed and how to get these.

The organisation has a number of DMI's trained across the force and in various departments. These can be utilised on a daily basis and the list of all DMI's is detail below.

[redacted]

Key Terminology: -

Antivirus - Software that is designed to detect, stop and remove viruses and other kinds of malicious software.

Botnet - A network of infected devices, connected to the Internet, used to commit coordinated cyber-attacks without their owners' knowledge.

Bring your own device (BYOD) - An organisation's strategy or policy that allows employees to use their own personal devices for work purposes.

Cloud - Where shared compute and storage resources are accessed as a service (usually online), instead of hosted locally on physical services.

Cyber-attack - Malicious attempts to damage disrupt or gain unauthorised access to computer systems, networks or devices, via cyber means.

Firewall - Hardware or software which uses a defined rule set to constrain network traffic to prevent unauthorised access to (or from) a network.

Ransomware - Malicious software that makes data or systems unusable until the victim makes a payment.

Two-factor authentication (2FA) - The use of two different components to verify a user's claimed identity. Also known as multi-factor authentication.

Denial of Service (DoS) - When legitimate users are denied access to computer services (or resources), usually by overloading the service with requests.

Digital footprint - A 'footprint' of digital information that a user's online activity leaves behind.

Encryption - A mathematical function that protects information by making it unreadable by everyone except those with the key to decode it.

End user device - Collective term to describe modern smartphones, laptops and tablets that connect to an organisation's network.

Internet of Things (IoT) - Refers to the ability of everyday objects (rather than computers and devices) to connect to the Internet. Examples include kettles, fridges and televisions.

Macro - A small program that can automate tasks in applications (such as Microsoft Office) which attackers

can use to gain access to (or harm) a system.

Patching – applying updates to firmware or software to improve security and/or enhance functionality.

Phishing - Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.

Software as a Service (SaaS) - Describes a business model where consumers access centrally-hosted software applications over the Internet.

Social engineering - Manipulating people into carrying out specific actions, or divulging information, that's of use to an attacker.

Spear-phishing - A more targeted form of phishing, where the email is designed to look like it's from a person the recipient knows and/or trusts.

Trojan - A type of malware or virus disguised as legitimate software that is used to hack into the victim's computer.

Water-holing (watering hole attack) - Setting up a fake website (or compromising a real one) in order to exploit visiting users.

Whaling - Highly targeted phishing attacks (masquerading as legitimate emails) that are aimed at senior executives.

Whitelisting - Authorising approved applications for use within organisations in order to protect systems from potentially harmful applications.

Zero-day - Recently discovered vulnerabilities (or bugs), not yet known to vendors or antivirus companies that hackers can exploit.

Digital Forensics Unit (DFU)

The Digital Forensics Unit deals with all manner of digital devices - Mobile Phones, Sat Navs, Tablets, Computers and storage devices. The DFU have the skills to safely examine, download and evidence the digital content from seized devices and where necessary can offer specialist support at the scene of an investigation. For further advice contact should be made with the unit direct.

Gloucestershire Constabulary

Intelligence guidance

Ver 2 June 2019 JL

To obtain the information included in this document in another language, large print or on an audio tape, contact the Communications and Engagement team on **01452 754466**

Gloucestershire Constabulary

Headquarters, No.1 Waterwells, Waterwells Drive, Quedgeley, Gloucester, GL2 2AN

www.gloucestershire.police.uk

/Gloucestershire.Constabulary

@glos_police