More Trust. Less Crime. High Standards.

Government Security Classification (GSC)	Official – Sensitive
Publication scheme Y/N:	No
Title:	Intelligence Reports Processing – Standard Operating Procedure
Version:	2.1
Author:	OCU Commander Andrew Featherstone DSU [redacted] PS [redacted]
OCU:	MO2 – Met Intelligence
Date:	05/02/2024

1. Purpose

The purpose of this document is to ensure MPS compliance with the National Intelligence Model (NIM) and College of Policing (COP) APP guidance on what constitutes intelligence and how intelligence will be processed. Furthermore, this document will ensure that all intelligence held by the MPS is compliant with legal frameworks, and that it is indeed intelligence. Relevant legal frameworks are:

- Computer Misuse Act 1990
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- Data Protection Act 1998
- Data Protection Act 2018
- General Data Protection Regulation

2. Guiding Principles

This policy aims to provide clear guidance on how intelligence is recorded, evaluated and disseminated with the implementation of CONNECT, with a particular focus on the following key areas:

- Submission of intelligence – what is (and is not) required from officers and staff.
- Triaging – how intelligence is reviewed, classified, actioned and prioritised.
- Evaluation – how intelligence is processed, how threat risk and harm is identified and managed.
- Dissemination – how intelligence is actioned, shared or developed. How we work with others internally, or collaborate with partners externally.
- How MO2 will interface via CONNECT, with other areas of the organisation.

3. Recording of Intelligence

Intelligence is defined within the National Intelligence Model as '*Information that has been subject to a defined evaluation and risk assessment process, in order to assist with police decision making*.'

All officers and staff submitting intelligence will be suitably trained and vetted to a level appropriate to their role, which will also reflect the access levels they have to police systems. The management and supervisor structures set above those officers and staff will have responsibility for ensuring the quality and consistency of their portfolios IR submissions. Information/intelligence reports should be submitted if it is believed its recording or dissemination is likely to advance any of the below aims:

- Interests of national security;
- Preventing or detecting crime;
- Preventing disorder;
- Protecting public safety or public health

Information must always be submitted at the earliest opportunity, ideally within the current tour of duty. Any information/intelligence reports that are submitted must be classified in terms of sensitivity in line with the Government Security Classification (GSC).

4. Intelligence Submission – All Staff

There are recognised roles within the CONNECT workflow for intelligence:

Submitting Officer – Is the originator of the intelligence report.

IRO (Intelligence Review Officer MO2) – Is the intelligence reviewing officer within the Intelligence Team who is processing the IR (Officer or staff equivalent).

Supervisor (MO2) – Is the supervisor within the Intelligence Team (Sgt or staff equivalent).

4.1 Roles and Responsibilities

The following outlines the core responsibilities for each of the recognised roles within the CONNECT workflow when submitting and processing intelligence. These actions MUST be completed as prescribed to meet APP (Authorised Professional Practice) compliance.

Submitting officer:

- PNC check (to confirm identity)
- CONNECT POLE search (to ensure intelligence is linked to the correct record)
- Create and link POLE records should none already exist
- Complete Question set THRIVE +
- Set MOPI levels
- Set NIM level
- Set handling conditions

IRO:

- Initial assessment check PNC check and POLE search been done;
- QA MOPI code;
- QA NIM level;
- QA Intel description;
- Review THRIVE+
- Add any relevant tags
- Add any relevant flags

- QA handling conditions

Note: For the first 6 months of CONNECT implementation the IRO will also complete a search on IIP to identify any other threat, risk or harm intelligence the submitting officer may not have access to. After this period the submitting officer will automatically see any relevant information which may influence their risk assessment at the point they conduct the basic CONNECT search, linking the POLE record and completing the THRIVE+ question set.

At the point the IRO has completed their role there are 4 options within the CONNECT workflow to complete the process:

1) **Accepted** – All IRO checks above have been completed.

2) **Return for correction** – If there is insufficient information to process the IR it should be returned to the submitting officer with directions on the remedial work required.

Note: IRs will only be retuned for fundamental issues such as unconfirmed identify (Is the individual named the same as the POLE record), no risk assessment completed. IRs will automatically be returned to the originating officers work tray for correction. Basic administrative errors will be corrected by the IRO. . If the IR requires further action being taken, such as the creation of a Crime Report, then the LIT will send the IR to the TCC CONNECT work tray, raising an action for the TCC to either complete the task or arrange for the task to be completed.

3) Return for deletion – Where information is not intelligence (see section 3 and 4.2) or no IR is required e.g. Duplication of information recorded elsewhere within CONNECT or other Met system; Information contained within crime reports, custody records, casefiles, referrals, stop checks, premises searches do not require an additional IR and MUST NOT be replicated. If the IR should be deleted an action is sent to the Supervisor for that LIT team. This will normally be the DS. Only DS or above have the authority to approve the deletion. This process ensures there is appropriate oversight and governance to the deletion of information.

Note: Stop search and premises records MUST be completed within the specific CONNECT tile and NOT on an IR. In these circumstances the IR will be deleted with an instruction for the submitting officer to follow the correct workflow. No-value intelligence will be assessed and actioned by the IRO with the rationale recorded within the IEL. IROs will ensure that any officers regularly submitting intelligence of no value, or where particular force processes are prompting high volumes of no-value intelligence are identified and escalated to the LIT DS.

***4*) Accepted and refer to Supervisor** – To be used by IROs who do not have direct submission status.

Note: Trained, competent IROs will have the autonomy for direct submission of IRs e.g. 'Accept and make live'. Trainee staff will always use the 'Accept and refer to Supervisor' until such time they are deemed competent to attain direct submission status. The process for accreditation will be at the discretion of the FLP Supt.

Supervisor:

The Supervisor in the relevant MO2 intelligence team will monitor the CONNECT 'Supervisor work tray' and is responsible for:

- Identify and task IRs for proactive 'Research & Development' by the R&D team using an 'action plan' (see Research section 6.4)
- QA IRs completed by IROs who have not achieved direct submission status (Initial assessment check PNC check and POLE search been done; check MOPI code; NIM level; Intel description; review question set THRIVE+; add any relevant tags; handling conditions);

- IRO has completed their checks Identified risk issues add actioned in action plan TCC (cell); apply any flags
- Progress IRs subject to Code C handling conditions

4.2 When not to submit an Intelligence Report

There is no requirement to submit an IR where:

- The submission does not meet the test of a legitimate policing purpose (outlined above); or
- The submission is a duplication of information already recorded elsewhere (in CONNECT under other POLE Cards or other Met systems) e.g. Crime reports CRIS, referrals MERLIN, incident reports CAD and custody reports; or
- The content relates to information that may be required to be shared, but does not constitute intelligence as defined in section 3; or
- When a stop search or premises search is completed the individual CONNECT tiles must be used.

4.3 Stop Search records

A record of a Stop Search will be created in CONNECT by the officer who conducted the search using the 'Create and Update' a 'Stop Search Event' tile. A separate IR is not to be created. An IR will not be used as an alternative to a Stop Search Record. In these circumstances the IR will be retuned for deletion and tasked back to the submitting officer.

If a vehicle is stopped with multiple occupants who are searched, a separate 'Stop Search Event' record must be created for each of the persons searched. Only the person in charge of the vehicle can be recorded on the same event as the vehicle.

If a vehicle is stopped with multiple occupants but not all are searched, the 'Person Present (Not Searched) Card' must be completed for those people that have not been searched. This Card can be added to the Card Index.

The submitting officer's line manager is responsible for completing any Supervisor Reviews and ensuring records are accurate and complete.

4.4 Premises Search records

A record of a Premises Search will be created in CONNECT by the officer who conducted the search using the 'Create and Update' a 'Premises Search Event' tile. A separate IR is not to be created. An IR will not be used as an alternative to a Premises Search Record. In these circumstances the IR will be rejected and tasked back to the submitting officer. 'Premises Search Events' should be linked to all relevant existing events on CONNECT by the submitting officer e.g. Investigation, Stop Search or Custody Record.

The submitting officer's line manager is responsible for completing any Supervisor Reviews and ensuring records are accurate and complete.

5. Completion of Intelligence Report

All IRs will be submitted via CONNECT and it is the user's responsibility to ensure that all submitted intelligence meets the Met Data Quality Standards. The process is outlined below.

1) The 'Create Intelligence Event' is opened from the home screen.
2) The submitting officer completes the following mandatory cards/fields, 'Basic details', 'Source', 'Intelligence summary', 'Providence' and 'Handling code'.
3) Add the details known to the Person/ Object/ Location (POL) where applicable and press 'next'
4) CONNECT will complete a search on the details provided and the officer/ staff either links or creates a new POL object.
5) The submitting officer completes the mandatory checks outlined in section 4.1.
6) The submitting officer selects and grades the Priority of the Intelligence Low/ Medium/ High.
7) The submitting officer will submit the intelligence report to the LIT that cover the relevant geographical MPS area (If there isn't one then the intelligence is submitted to RED day under process FS.8.1.3.08 RED Day - Intel Supervision).

At the time of submission the Submitting Officer will grade the intelligence based upon their own professional judgement as either Low / Medium / High priority. If the IRO is unsure of the level of priority that should be attributed to an IR they should seek advice from their immediate line manager.

5.1 Priority definitions

Low – Other information

Medium – NIM Control Strategy. Intelligence Requirement/Current OP/Tactical;

High – Risk of Serious Harm

All intelligence will be assessed and disseminated in line with the NIM (National Intelligence Model).

5.2 NIM Levels

The submitting officer will need to select one of the three recognised NIM levels the intelligence relates to:

1) Local or Basic Command Unit
2) Force and or Regional
3) Serious and Organised Crime Usually National or International

5.3 Data Quality Standards

It is the responsibility of the submitting officer to complete the checks outlined in section 4.1. It is imperative the question set THRIVE + is completed by the person who is submitting the intelligence and best placed to make the assessment.

The purpose of these checks, is for the submitting officer to identify and manage risk; and add value to the intelligence being submitted, taking in account the wider known information about the person, persons, location or event. It must be remembered by the submitting officer that the purpose of intelligence is to drive activity.

5.4 Professional Curiosity

Minimum standards include submitting officers exercising professional curiosity on all occasions when submitting an IR. The below is a non-exhaustive list of questions the submitting officer should be asking prior to submission:

- Is there an indication that the people or vehicles included in the report feature in other BCU or force areas?
- Have the minimum checks revealed any of the people in the report are currently wanted or missing?
- Have the minimum checks revealed an action should be taken in relation to the vehicles in the report?
- Does the report highlight vulnerability concerns, including domestic abuse, child sexual exploitation, child criminal exploitation or other concerns such as truanting?

In the event that the answer to any of the above questions is 'yes', it is for the submitting officer to take the appropriate course of action, which should be referenced within the intelligence report. It is important to stress that professional curiosity is everyone's responsibility. Please refer to your supervisor if unsure on what action to take.

5.5 Threat & Risk Management

The submitting officer is responsible for identifying and managing threat, risk and harm using the THRIVE principles before submitting information/ intelligence on an IR. It is imperative submitting officers understand the role of MO2 is limited to processing intelligence and not one of risk management or provide a 'safety back stop' for any particular department. Only in circumstances of unmanaged clear, real and immediate threat to life or property, as described in the body of the intelligence submitted will remedial action be taken by MO2. In this event, contact will still be made with the Submitting Officer, their Supervisor and the TCC to highlight the nature of the risk that was not managed and to ensure repetition does not occur.

6. Performance & Governance

It is essential that the implementation of CONNECT is seen and embraced as an opportunity to raise the standards of intelligence reporting across all areas of Front Line Policing and preserve the integrity of the information held within CONNECT. The primary role of MO2 is to process and disseminate high quality actionable intelligence and will include continued monitoring of quality assurance. The repeated submission of substandard IR's by individuals will be tracked and highlighted by the LITs and will be dealt with by following an incremental staged improvement process which will include feedback, mentoring, line manager escalation and action plans. Repeated failures by one particular unit or strand will be escalated to the Superintendent strand lead for the BCU/ OCU.

6.1 Structure & Format

All 3x5x2 information/ intelligence reports submitted should emphasise quality over quantity and adhere to the prescribed guiding principles:

- **Accuracy**: All information submitted should be accurate, including source attributions; where doubt exists, additional efforts should be made to verify the accuracy of the information. Inaccurate information/intelligence reports should not be submitted; in the event that it is, it should be deleted.
- **Actionable**: The information submitted should have the potential to lead or contribute to further development and policing action.
- **Adequacy:** The information submitted should be of sufficient detail taking in to account the purpose for which it is being submitted. Inadequate intelligence reports should be

returned to the person submitting for additional information to be added.

- **Duplication**: The information should not be submitted if it is already recorded on another MPS system unless it adds further details and value.
- **Relevance**: The information must be relevant to the policing purpose for which it is being submitted.
- **Timeliness**: Intelligence should be submitted, wherever possible, during the current tour of duty and otherwise within 24 hours.

Regular data quality assurance checks and compliance with this policy will be conducted by the Force/BCU Intelligence Management Unit Manager (MO2) on reports received and processed within the Force.

6.2 Source

The source of the information can be both the name and address of the person providing the information or an intelligence source reference (ISR) number.

To minimise the risk of compromise, details of the source must not be placed in the main body of the report, and the identity of the source must not be available to operational officers and staff. The report must have a unique reference number (URN) assigned to it. A second, sanitised version of the report will be created by the intelligence unit if editing or sanitisation is required.

Items of information from the same source but concerning separate matters should be recorded on separate IRs to prevent inadvertent identification of the source. Submission of separate IRs should also be considered when the source provides more than one item of information on the same matter. Intelligence will only be accepted from key partners and stakeholders using the 3x5x2 submission format.

6.3 Grading

All information/intelligence reports will be graded using the 3x5x2 system. This is to allow MO2 to assess, develop and disseminate the intelligence, confident that wider implications and risk have been considered by the IRO.

- Source Evaluation
- Information/Intelligence Evaluation
- Handling Code
- And the usability of the information, in the opinion of the submitting officer – confirmed by the IRO

Source Evaluation

The source will be evaluated as one of:

1) **Reliable:** The source is believed to be competent and the information received is generally reliable. This may include information from human intelligence, technical and scientific sources.
2) **Untested**: The source has not previously provided information to the person receiving it or has provided information that has not been substantiated. This is not to say that the source is necessarily to be viewed as unreliable.
3) **Not reliable**: There exist reasonable grounds to doubt the reliability of the source, which should be documented within the information/intelligence report risk assessment. Such grounds may include concerns regarding the authenticity, trustworthiness, competence or motive of the source.

Information/Intelligence Assessment

The information/intelligence will be assessed as one of:

A. **Known directly:** The source has obtained the information first-hand, such as through witnessing it.
B. **Known indirectly but corroborated:** The source has not obtained the information first-hand but the reliability of the information/intelligence can be verified by separate information that carries the information/intelligence assessment of A.
C. **Known indirectly:** The source has been told the information/intelligence by someone else and has no first-hand knowledge of it.
D. **Not known -** There is no means of assessing the information. Information/intelligence from an anonymous source or Crimestoppers would receive this assessment.
E. **Suspected to be false:** Irrespective of how the source obtained the information, there is a reason to believe the information is false. The rationale for this belief should be documented in the information/intelligence report risk assessment.

Handling Codes

The information/intelligence handling will be one of:

P. **Lawful sharing permitted**
C. Lawful sharing permitted with conditions

Handling code P will be the default value.

6.4 Research (Intelligence Professionals Only)

The basic principle is that all IRs require processing, however, not all IRs require further research. The level of research applied to each IR will vary depending on its value, usability or unmanaged risk. Intelligence logs being evaluated will be researched, linked and categorised as per table in section 6.5. The guiding principles will be informed by local and MPS wide operational priorities, as well as unfolding operational risks, or incidents. Each BCU Intelligence Manager will be expected to have a detailed understanding of how their teams capability and resources can be used best to support those priorities. The intelligence manager will be expected to craft his or her local intelligence collection, and development plan in order to service the daily BCU operational rhythm, and the tactical tasking process via the TTCG.

6.5 Usability

The IRO will review the IR in order to assess usability, in line with local and strategic priorities. The IR's assessed usability will influence to what degree the IR is further developed / and or disseminated.

A – Actionable: Actionable intelligence is a single piece of intelligence that affords the opportunity for positive action, in terms of arrest, warrant execution, the location of a person of interest or the recovery of property

D – Developmental: Where further research and development is required which could include the development of intelligence products. Making the decision not to do anything at this point in time, but subject to review at a future date.

I - Intelligence Value: Used for routine day to day information relating to people of note, vehicles, addresses and locations or incidents that have occurred in the past.

N - No intelligence value: Used where after review and assessment the information does not have a policing purpose or is not proportionate to record, is incorrect, or duplication.

Usability	Research	Linking	Dissemination
Actionable	Proactive research	All entities linking.	LIT R&D (BIDO)
Developmental	Proactive research	POLE linking only.	LIT R&D (BIDO)
Intelligence Value	Basic IRO processing	POLE linking only.	No onward dissemination.
No Intelligence Value	None.	None	Return for rework

Where an IRO identifies a clear breach of policy or serious risk to life they will flag the IR to the LIT DS for review and further action, the LIT DS will then escalate to the BCU TCC.
Action plans can be generated from any IR by any officer or staff member, once processed the IRO can take the decision to refer the IR to another officer or teams 'CONNECT Tray', whilst simultaneously raising an action for the recipient. The officer will update the action plan with the necessary details. If the officer is unable to complete the action plan (e.g on AL/ rest day/sick etc.) than any officer can access their work tray and complete the action plan on their behalf. The LIT team will then receive the update on the action plan. The action plan details is logged on the IR and is visible to all users. Throughout this process the IR is visible to all users on CONNECT. It will not upload to PND until the assessment process is complete and the report is LIVE.

6.6 Evaluation and Quality Assurance of IRs (Intelligence Professionals Only)

Evaluating IRs is a key function of MO2 conducted by the IRO and is necessary to sort quality intelligence from inappropriate submissions and provide feedback to officers to raise quality standards. The IROs are not expected to return intelligence for amendments that can be resolved by minor research, or where processing the information is more critical than waiting for a Submitting Officer to amend a report. Once an IR has been received by the intelligence unit, the IRO will complete the checks outlined within the 'Roles and Responsibilities' section 4.1:

- Intelligence value
- Accurate and full provenance of the information
- Consideration for further research and development
- Quality assurance of data standards
- Consideration for dissemination and requirements for sanitisation
- Risks and duty of care issues

Any amendment to the report should have an audit trail. This may include the resubmission of a sanitised IR linked directly to the original report.

The person recording the report should be considered as credible with regards to the source reliability and information evaluation unless there is an obvious discrepancy or incompatibility. The person who submitted the report should be contacted if further clarity or corroboration is required on any issue

6.7 Evaluation Timelines

IRs need to be processed in a timely and efficient manner. Target timelines for processing will be based on their priority grade which are as follows:

Priority Grade	Target
High	Within 24 hours of triage
Medium	Within 72 hours of triage
Low	Within 14 days or as soon as practical depending on other demand

A snapshot of demand across the intelligence units will be conducted once per day at 0800 in order to establish demand and track productivity. Demand will be viewed within a force context as well as a BCU/OCU where resources will flex across departmental and geographic boundaries to meet demand via tasking at the DIM.

6.8 Handling Code C

All intelligence reports are required to have one of the following codes:

P – Lawful sharing permitted
C – Lawful sharing permitted with conditions

All intelligence with a handling code of C should be reviewed regularly in order to ascertain whether the handling grading still applies or if the information should be re-graded to P to allow lawful sharing of the intelligence. There are two types of Code C reviews; Ad-hoc and scheduled. Ad-hoc reviews can be performed by intelligence professionals at any point and is typically completed in instances of high-risk intelligence. A scheduled review is performed when the due date of the Code C review is reached.

Handling code C should only be used by specially trained officers.

When handling code C is applied, the receiving agency must observe conditions specified by the originator. A risk assessment may be required. Should the intelligence be used in court proceedings, an application for public interest immunity should be considered. The recipient must abide by the handling conditions and must contact the recipient before conducting any activities outside of the conditions. If a report has handling conditions attached, they should be kept under review as there may come a point when they are no longer applicable and the intelligence report may be shared more widely, such as at the conclusion of an operation.

6.9 Append Information

Additional information can be added to an IR by performing the action Append Information. Information is added to the intelligence text on the 'Intelligence' card. Adding information does not replace existing information.

6.10 Updating IRs

MO2 staff with relevant permission can update an intelligence report by performing the 'Update Intelligence Report' action in CONNECT. The Management of Police Information (MOPI) grouping can be amended using the MOPI Grouping Amendment action in CONNECT. It is critical the MOPI group is proportionate to the nature of the intelligence and is assigned correctly. Further guidance on MOPI grouping can be found here Review, retention and disposal | College of Policing

https://www.college.police.uk/app/information-management/management-police-information/retention-review-and-disposal#review-schedule

6.11 Sanitising IRs

The removal of Intelligence source details and provenance will take place during the sanitisation process completed by the IRO. The information contained within the submission will be sanitised to remove information which may reveal the identity of the Intelligence source or disclose police methodologies. Intelligence professionals have permissions to update or amend any POLE card within the CONNECT record. Any concern or uncertainty relating to the IR sanitisation process, should be escalated to an MO2 DS or Intelligence Manager.

6.12 Dissemination of IRs

The IRO will complete an initial assessment with regard to the dissemination requirements of the sanitised intelligence occurrence and disseminate as appropriate via CONNECT. Consideration will be given as to whether the IR requires dissemination to a specific operational Command; Unit; Operation; Officer or Briefings Team in support of the Control Strategy Priorities, persons of note or to minimise / mitigate risk. The LIT DI (Intelligence Manger) will responsible for the creation and accuracy of the dissemination lists relevant to their BCU or OCUU.

Lawful Sharing Permitted (P)

Dissemination to European Economic Area (EEA) law enforcement agencies is permitted without any additional information/intelligence report risk assessment. Dissemination to non-EEA law enforcement agencies should be subject to a risk assessment. Under the Data Protection Act 1998, personal information may be disseminated outside of the EU only after the risks have been assessed and on the grounds of substantial public interest. In this context, public interest will include tackling serious and organises crime, and the maintenance of the security and integrity of law enforcement agencies. Additional care should be taken when handling information/intelligence from HMRC, as further unauthorised dissemination risks the commission of a criminal offence. In the event this is likely, HMRC will provide a warning within the report.

Sharing With Conditions (C)

When handling code C is applied, the receiving agency must observe conditions specified by the originator. A risk assessment may be required. Should the intelligence be used in court proceedings, an application for public interest immunity should be considered. The recipient must abide by the handling conditions and must contact the recipient before conducting any activities outside of the conditions. If a report has handling conditions attached, they should be kept under review as there may come a point when they are no longer applicable and the intelligence report may be shared more widely, such as at the conclusion of an operation.

The approved conditions, as listed by the COP APP, are as follows:

- **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 derived intelligence.
- **A2 Covert Use** Covert action may be take on this intelligence, though the source, technique and 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 as specified by the source intelligence owner.
- **S1 Delegated Authority** Originator of intelligence permits the unsupervised sanitisation of the material in order to allow dissemination to a wider audience.
- **S2 Consult Originator** Originator of intelligence does not permit sanitisation of the material for wider dissemination without consultation being sought.

The incorrect sharing of Intelligence presents a significant Risk for the organisation, any sharing of intelligence outside to an outside agency by LIT staff MUST be authorised by the

BCU Intelligence Manager or the MO2 on-call DI.

6.13 Risk Assessment

The incorrect sharing of intelligence can pose a significant risk to person, persons and the organisation. The sharing of intelligence needs to subject to oversight and risk management. The risk assessment undertaken needs to be commensurate with the nature of the intelligence to be shared and the status of the person, or organisation the intelligence is being shared with. The risk associated through the routine sharing of intelligence between UK Law Enforcement Agencies (Policing / NCA) will have been subject to an initial risk assessment process via the application of 3x5x2 process and handling conditions.

If handling code C has been applied to intelligence that is to be shared with UK Law Enforcement agencies, then the officer/ staff member should highlight to the recipient the nature of the attached conditions, and record this on the IR CONNECT activity log. If the officer or staff member seeking to share intelligence has any concerns around the associated risk, then he or she should seek guidance from the BCU Intelligence Manager or the on-call MO2 LIT DI. For guidance purposes – Decision making considerations can be found on Met Form 5020C

If intelligence to be shared is deemed sensitive due to nature of origin, it's potential to reveal covert policing techniques or any wider concerns re the potential impact of handling conditions, then the officer or staff member should seek advice from BCU Intelligence Manager or MO2 Sensitive Intelligence Unit [redacted]
When seeking to share intelligence with overseas Law Enforcement partners, consideration to be given to obtaining advice from the JICC (Joint International Crime Co-ordination Centre) ,and reviewing the FCDO – Principles *The Principles relating to the detention and interviewing of detainees overseas and the passing and receipt of intelligence relating to detainees*

http://mpsweb.intranet.mps/news-archive/features/2019/march/international-crime-coordination-centre-iccc-met/

On all occasions that intelligence is to be shared outside of MPS CONNECT network, the officer should default to using the internal CONNECT 'Risk Assessment' Tile. This is completed by the user prior to disseminating an IR externally. It replicates similar functionality on Crimint. The risk assessment is logged on the IR in the task history. Once the risk assessment has been completed, the user can then complete the 'External Dissemination' by using the 'Media Manager' card. The IR is generated in PDF format. Additional handling questions must be completed for the receivers benefit. The report is the emailed within CONNECT. This is logged on the IR. This removes the need to create a separate IR just to log the details of information sharing, as is the current practice on Crimint.

6.14 Audit Logs

All action taken in relation to the processing and decision making for each IR will be recorded on the CONNECT audit record and where necessary action log. This is to include the rational for decisions taken and disseminations. The 'Log of Enquiry' card. This is a decision log which is available on all event types. It will be used in an equivalent way to the Supervision Tab on Crimint. Visibility is limited to just Intel users and Inspectors and above to allow more sensitive information to be recorded. It won't need as much detail added to it as on a Crimint as all activity (e.g. Action plans, disseminations etc.) are logged on the task history with full details visible. This improves supervision, scrutiny and accountability.

LIT DSs will routinely dip-sample completed evaluations to ensure standards are being maintained, and to help identify any knowledge gaps and training requirements. Ideally at least 1 log per IRO per week will be reviewed. All actions taken during the evaluation process, alongside relevant notes and comments, will be recorded within the relevant

section of the CONNECT IR. Supervisors can review and evaluate the Government Security Classification (GSC) marking of the Intel report. This will default to 'Official'. This can be changed as required by selecting the 'Pen' icon in the top right of the Intel report. The following options can be selected (Official, Official Sensitive and Official Sensitive – non-PND). Once their review is complete, Select 'Add New Log of Enquiry'. On the Log the LIT supervisor will document the rational and decision making. This will include any relevant further research and development and rational for onward dissemination.

6.15 Category Cards

The 'Category' card is used when there is insufficient data to create a POLE record to the IR. All IR's must have at least one POLE record linked to them in order for the assessment process to be completed. The 'Category' card is only available for intelligence users at the point of assessment and allows for data such as nick names to be recorded i.e 'Intel suggests that nickname 'MOUSE MAT' has access to firearms.' insufficient data for a person or location POLE to be added at the point of submission. Access is limited to intelligence users only to ensure correct usage of this feature. It will be the responsibility of the IRO completing the initial to identify the IRs that require the creation of a 'Category' card, once identified the officer will then generate the relevant 'Category' card.

Example – Intelligence Reporting indicates that a male named Steve G is dealing drugs in South Norwood. As the details contained in the report are insufficient to complete a POLE record for Steve G. The IRO would generate a Category card so all further reports referring to Steve G can be linked. Should full details be later obtained, then a full POLE record will be generated.

6.16 Other POLE Entities

All phone numbers mentioned in the intelligence text should also be recorded on a 'Communications' POLE card, in the same way as a person, vehicle or location is. It is an optional card which is added to the list at the point creation by the submitting officer. It can then be linked to any event type including IRs and PMP's. The Communications card also allows for any communications types to be included. E.g. Email address, IMEI numbers, social media handles and IP addresses. All IRO's submitting an IR that contains one of the aforementioned unique identifiers must complete the relevant 'Other' POLE entity record" so as to ensure that selectors such as telephone numbers can be linked to multiple POLE records should the need arise.

Example – T8246 is identified as a County Line Telephone number, this number should be created as another POLE entity, so the number can be linked to the POLE records of multiple line holders