Ministry of Defence Police

[redacted]

Freedom of Information Manager

Ministry of Defence Police

Palmer Pavilion,

Building 666,

RAF Wyton, Huntingdon,
Cambs, PE28 2EA

Telephone: +44 (0)1371 85[redacted]

E-mail: MDP-FOI-DP@mod.gov.uk

Our Ref: eCase: FOI 2022/03452

RFI: 061/22

Date: 8 April 2022

Dear [redacted]

FREEDOM OF INFORMATION ACT 2000: MINISTRY OF DEFENCE POLICE: RECORDING OF SEX/GENDER.

We refer to your email dated 10th March 2022 to the Ministry of Defence Police which was acknowledged on the 15th March 2022.

We are treating your email as a request for information in accordance with the Freedom of Information Act 2000 (FOIA 2000).

In your email you requested the following information:

This is a FOIA for the following information. Please provide separate answers to the following 8 questions in respect of Crime & Incident Reporting:

1. What explanatory guidance has been provided to your police force on the information you should record in the 'gender/sex' category? As examples, this might include guidance documents provided by: College of Policing, Home Office, ONS, or any other official body. Please provide me with a copy of the guidance document(s) in use.

2. In the gender/sex category does your police force record a victim's or suspect's "natal sex" (their biological sex observed at birth), their "legal sex" (the sex on their birth certificate), or their "self-declared gender or gender identity"?

3. If a male-born person self-identifies as female will this be recorded by you as female or male?

4. If a male-born person self-identifies as non-binary will this be recorded by you as female or male or something else?

5. If someone is transgender (identifies as a different gender to the sex assigned at birth) and has obtained a Gender Recognition Certificate is this recorded by you separately?

6. If someone is transgender (identifies as a different gender to the sex observed at birth) but has not obtained a Gender Recognition Certificate is this recorded by you separately?

7. If a male-born person identifies as female, has obtained a Gender Recognition Certificate and is arrested for/charged with the crime of rape will you record the gender/sex of the suspect/perpetrator as male or female? Will transgender status also be recorded?

8. If a male-born person identifies as female, has not obtained a Gender Recognition Certificate and is arrested for/charged with the crime of rape will you record the gender/sex of the suspect/perpetrator as male or female? Will transgender status also be recorded?

Additionally, please answer the following:

The College of Policing requirements for Information Management specify that each UK police force must have an Information Management Strategy (IMS): Common process

Common process - As you will know, the IMS should be made available to partners and the public, and I would therefore ask you to please provide me with a copy of your local police force IMS.

A search for information has now been completed by the Ministry of Defence Police and I can confirm that we do hold information in scope of your request.

Please note: The Ministry of Defence Police are not part of the Annual Data Requirement scheme.

Incident and Crime recording

1.What explanatory guidance has been provided to your police force on the information you should record in the ‘gender/sex' category? As examples, this might include guidance documents provided by: College of Policing, Home Office, ONS, or any other official body. Please provide me with a copy of the guidance document(s) in use.

No information held

In respect of questions 2 to 8, Information is defined in section 84 of the Act as 'information recorded in any form'. The Act therefore only extends to requests for recorded information. It does not require public authorities to answer questions generally; only if they already hold the answers in recorded form. The Act does not extend to requests for information about policies or their implementation, or the merits or demerits of any proposal or action - unless, of course, the answer to any such request is already held in recorded form." (Day vs ICO & DWP – EA/2006/0069 Final Decision)

Additionally, please answer the following:
The College of Policing requirements for Information Management specify that each UK police force must have an Information Management Strategy (IMS): https://www.app.college.police.uk/app-content/information-management/management-of-police-information/common-process/#-common-process-at-force-level
As you will know, the IMS should be made available to partners and the public, and I would therefore ask you to please provide me with a copy of your local police force IMS.

Please see attached document which is currently under review and subject to being updated in due course.

If you have any queries regarding the content of this letter, please contact this office in the first instance.

If you wish to complain about the handling of your request, or the content of this response, you can request an independent internal review by contacting the Information Rights Compliance team, Ground Floor, MOD Main Building, Whitehall, SW1A 2HB (e-mail CIO-FOI-IR@mod.gov.uk).

Please note that any request for an internal review should be made within 40 working days of the date of this response.

If you remain dissatisfied following an internal review, you may raise your complaint directly to the Information Commissioner under the provisions of Section 50 of the Freedom of Information Act. Please note that the Information Commissioner will not normally investigate your case until the MOD internal review process has been completed. The Information Commissioner can be contacted at: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. Further details of the role and powers of the Information Commissioner can be found on the Commissioner's website at https://ico.org.uk/.

Yours sincerely

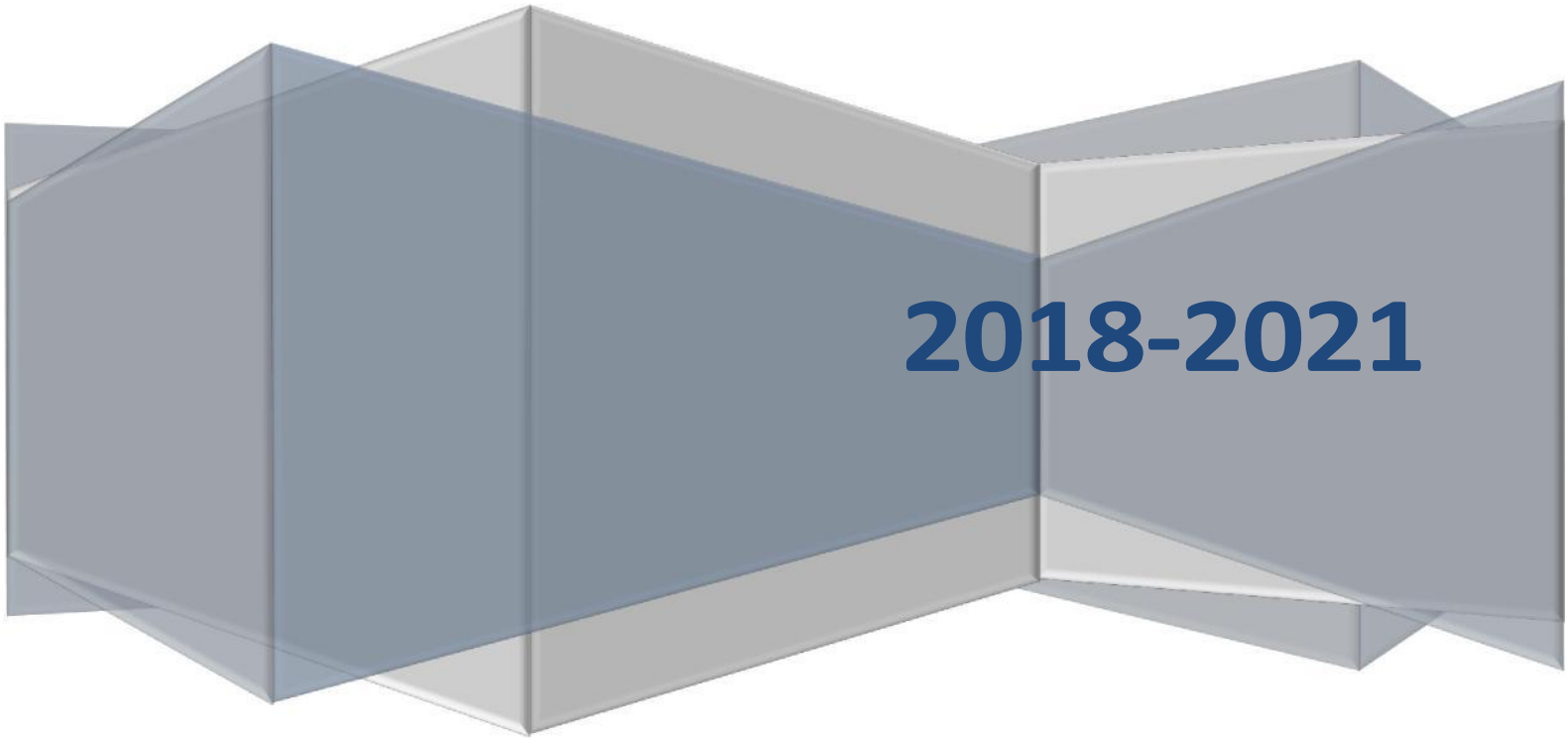
MDP Secretariat and Freedom of Information Office

Ministry of Defence Police

Strategy and Improvement Plan

Owner: Senior Information Officer
Author: Force Information Manager

20180927-MDP_RecordsManagementStrategyImprovementPlan_v0.1



Contents

1. Records Management Improvement Strategy

1.1 Our Intent

We acknowledge the importance in the digital age of managing the lifecycle of our records, both physical and electronic, through effective records management practices.

We therefore commit to improving records management to ensure our records are managed throughout their lifecycle in a systematic, cost-effective and efficient manner.

Good records management ensures our records, in any format, are readily available for use, and sharing with partner agencies, so we will be meticulous in our control environment so that our records maintain their authenticity, availability and integrity.

Compliance with an improved control environment will:

- contribute towards the avoidance of significant risk to the force by enabling and providing evidence of transactions and decision making;
- reduce vulnerability to legal challenge;
- support proper control of storage and volume of records to reduce costs in finding and managing them; and
- promote best value in time and resources.

It is our intention to implement seven key principles that will help us achieve the best control environment and drive improvement in our records management culture.

Embedding these principles in our day to day business will provide a foundation from which we can demonstrate our commitment to meet the highest standards in records management and provide a beacon of best practice for others to follow.

1.2 Our Principles

Principle of Accountability

A senior responsible officer shall oversee the records management function including delegating responsibilities and this will be documented in a manner that is verifiable and available to all.

Principle of Competency

Principle of Compliance

Principle of Confidentiality

Principle of Integrity

information generated or managed by the force are credible with a reasonable

Principle of Availability

The force shall maintain records in a manner that ensures the right information

Principle of Transparency

2. Current Situation and Next Steps

This section will describe where we are with our records management and recommend the next steps to achieve compliance with our Records Management Principles.

2.1 Principle of Accountability

2.1.1 Senior Responsible Officer

Current Situation – The force has appointed the Head of Operational Standards as the Senior Information Officer (SIO) with responsibility for overseeing the records management function and standards in information management. The SIO is accountable to the Deputy Chief Constable as the force Senior Information Risk Owner (SIRO) and reports on information and records management issues to the Information Management Group (IMG).

Next Steps – Completed (Evidence of completion - MDP Information Management Plan 2018-21)

2.1.2 Delegated Responsibilities

Current Situation – Key roles and responsibilities have been established and identifiable police and civilian personnel have been allocated to those positions. Information Asset Custodians have been appointed by Information Asset Owners to oversee day to day requirements of managing their information assets and records.

Next Steps – Completed (Evidence of completion - MDP Information Management Plan 2018-21)

2.1.3 Governance Structure

Current Situation – The key information management functions, component activities and associated transactions of the force is contained in the Information Management Plan 2018-21 and was developed and signed off by the SIRO at the Information Management Group (IMG) meeting in December 2017, following consultation with key stakeholders across the force (Evidence in published minutes of IMG meeting 8 Dec 17). The IMG chaired by the SIRO and attended by senior managers and IM professionals is the top-level group for oversight of information management within the force (Evidence in published terms of reference and minutes of meetings). Beneath this sits the Information Systems Steering Group (ISSG) chaired by the Assistant Chief Constable for Organisational Development and Crime (ACC ODC) and below this are several working groups with specific remits. These are the CIS Security Working Group (CISSWG) which deals with systems security issues, the Information Assurance Group (IAG), which deals with assurance issues, and the Information Exploitation Group (IXG), which deals with how we use information. The IMG, ISSG and CISSWG meet quarterly, but the IAG and IXG have not met for some time due to staff transfers and other competing priorities.

Next Steps – It is recommended the IAG and IXG review their terms of reference and commence regular meetings to complete the information governance arrangements.

2.2 Principle of Competency

2.2.1 Records Management Professionals

Current Situation – The key roles in records management have been identified and are filled (or undergoing recruitment), however, the core competencies, key knowledge and skills required by these staff are not clearly defined leaving staff with key roles to complete ad-hoc courses to meet perceived needs alongside mandatory training. Clarification is required to demonstrate key staff understand their roles and responsibilities and can provide expert advice and guidance.

Next Steps - It is recommended (a) records management be identified as a distinct stream within the force training portfolio, and (b) essential training and development be identified within role profiles for key staff as part of a comprehensive continual professional development process.

2.2.2 All Personnel

Current Situation – The Defence Information Management Passport (DIMP) is the mandatory on-line information and records training for all personnel with Version 5 released earlier this year.

[redacted]

Next Steps – It is recommended (a) Chronicle is used to record mandatory records management training and, (b) the force information management site collection on MODNet is used to provide a one-stop shop for all records management needs and links to training.

2.3 Principle of Compliance

2.3.1 Legislation

Current Situation - The force has a legal obligation to comply with the General Data Protection Regulations (GDPR) and Data Protection Act 2018 which came into effect in May 2018 and new requirements are being included in our records management process. The force needs an up to date Data Protection Policy to demonstrate our commitment to compliance accompanied by easily accessible guidance to staff on their responsibilities for the processing of personal data.

Next steps – It is recommended a new Data Protection Policy and guidance is provided to all staff in an easily accessible format to raise awareness of their responsibilities in processing personal data.

2.3.2 National and Departmental Standards

Current Situation – Since 2014 the force has had Level 3 compliance under the Information Assurance Maturity Model (IAMM). MOD still uses the discontinued IAMM but departments such as MDP and DBS have not been included since 2017. This has left the force without a definitive

set of measures against which to assess maturity. NPCC has set up a data quality portfolio and it is likely this will set maturity standards to meet the needs of the NLEDS Programme.

Next Steps – The force should maintain its momentum in aspiring to achieve high standards by engaging with other forces through the NPCC Data Quality portfolio and establishing a credible maturity matrix for records management internal assurance audits and processes.

2.3.3 Force Policies and Procedures

Current situation – The MDP Information Management Directive issued in December 17 provides the overarching statement of our information management principles and includes making sure we have the right governance regime in place to meet compliance with legislation and national standards. The policies and procedures in place for records management have not been reviewed since GDPR and the Data Protection Act 2018 were introduced and are being refreshed to capture the new requirements.

Next steps – It is recommended force policies and procedures for records management are informally reviewed at least annually by the Force Information Manager, to ensure they remain relevant and up to date, with a formal review alongside key stakeholders and subject matter experts every 3 years.

2.3.4 Audit and Assurance

Current Situation – There is evidence of transactional audits, such as PNC and PND activity, and local assurance by line managers reviewing and signing officers pocket notebooks and crime files, but little assurance reporting during the year on whether records keeping meet standards. It is recognised this is unsatisfactory, and an updated records audit and assurance regime should be implemented.

Next Steps – It is recommended the force identifies assurance standards for records management and puts in place a transparent process that reports to the SIRO through the Information Assurance Group.

2.4 Principle of Confidentiality

2.4.1 Protective Marking

Current Situation – The force has adopted the Government Security Classification (GSC) for marking its records.

Next Steps – It is recommended the force includes compliance with GSC across the force as part of its records management maturity matrix and assurance process.

2.4.2 Access Controls

Current Situation – [redacted]

.

Next Steps –

2.4.3 Security Architecture

Current situation – There are several information security policies and procedures to protect information and systems from unauthorised access, use, disclosure, disruption, modification, or destruction. These are over 5 years old and should be reviewed to make sure they remain relevant in light of the latest security threats and be subject to audit to check compliance.

Next steps – It is recommended that the security policies and procedures are reviewed to make sure they remain relevant and are being applied uniformly across the force. They should then be reviewed informally at least annually by the IT Security Officer, and formally every 3 years by the IT Security Officer and other key stakeholders and subject matter experts.

2.5 Principle of Integrity

2.5.1 Audit Trail

Current situation - Like many organisations, the force's commitment to manage the audit trail of its records has not necessarily translated into an ability to execute this in practical terms. Audit trail information for paper-based records is largely missing, although the author and target audience is sometimes available, while in the electronic environment the use of metadata is fragmentary when covering document naming and use of version control. Since the force creates records for both organisational and policing purposes it will be challenging to manage all records created within different electronic records management systems, however, it is good practice to use metadata alongside the retention and disposal schedule so that audit trail information is accurately captured.

Next steps – The force should look to improve the management of electronic records within its current systems by providing guidance to staff on the use of metadata, document naming and version control.

2.5.2 Data Quality

Current Situation – [redacted]

Next Steps – It is recommended the force (a) agrees and applies consistent terminology for the creation of policing records, and (b) uses the migration to MODNet as an opportunity to cleanse records holdings to remove duplicates and earlier versions.

2.6 Principle of Availability

2.6.1 Electronic Records and Document Management

[redacted]

Current Situation –

[redacted]

While understandable based

[redacted]

Next Steps - It is recommended that if a clear requirement for an electronic record and document management system is to be developed, a Project Board should be established to oversee the project and report back throughout delivery.

2.6.2 E-Mail records

Current Situation – E-mail records are managed inconsistently but need to be treated like any other record. Many transactions and decisions are commonly recorded in e-mail messages and it is important these are captured as records at the appropriate stage. The widespread and often informal use of e-mail means messages with policing and corporate value are frequently sent and received alongside many others of temporary or inconsequential value. E-mails that are trivial or have no long-term value should be deleted as soon as possible as we are retaining e-mails containing personal data which are subject to the Data Protection Act 2018 which requires personal data to be kept for no longer than necessary. Users need to know how to differentiate between these and recognise whose responsibility it is to capture relevant e-mails within the force's record keeping system. It is also a concern that with lack of guidance there may be e-mail records in personal mailboxes which are less accessible to the wider organisation and run the risk of being lost. The common practice of attaching documents to e-mails exacerbates the problem of multiple versions of the same records. Instead of attaching the document to an e-mail message, which will provide each recipient with an individual copy, a version of the document should be placed in a shared workspace. Recipients can then be directed to retrieve the document by including a pointer or link in an email message, which will lead the recipient to the master version. Distributing documents in this way helps encourage a culture of information sharing within the force and reduce the number of working copies of documents in disparate user folders.

Next Steps – It is recommended the force adopts a consistent approach to the management of email to ensure that relevant e-mail records are not lost.

2.6.3 Criminal Justice System Common Platform

Current Situation – National policing continues to implement a digital first strategy to manage investigation material within the criminal justice system on-line through a common platform. This includes case files and exhibits such as recordings from BWV and CCTV as well as digital interview recordings being electronically available to the prosecutor, and disclosure material being available electronically to defence legal teams. The force is some way behind other forces particularly when using custody facilities which have switched to digital interview recording.

Next Steps – It is recommended the force explores opportunities to reduce reliance on hard copy records in the criminal justice system and move to digital records wherever possible.

2.6.4 Physical Records Management

Current Situation – The Review, Retention, and Disposal Unit (RRDU) has two members of staff allocated to storing and managing both policing and organisational physical records, e.g. paper files, audio tapes, DVD's and CD's, and facilitating access to those records. The RRDU facility comprising which store crime and intelligence files, tapes, and other media are nearing maximum capacity, which store organisational records are at maximum capacity. There remains a huge volume of boxes containing unstructured files and records which adds to the problems such as records being retained longer than necessary; capacity issues within the facility; lack of intellectual control over the records; and health and safety risks to staff.

Next Steps - It is recommended the force reviews its management of unstructured records alongside its physical records needs and service provision. This should recognise Project Jute and include specific emphasis on facility design and location, staffing, resources, and procedures.

2.6.5 Business Continuity and Vital Records

Current Situation - Business Continuity Plans must include measures to ensure the force's key records and systems are protected and made available as soon as possible in the event of an emergency. The introduction of relatively new IT systems recently, such as Chronicle and the Global Rostering System, as well as upgrades to some of our Capita products such as Control Works and Unifi suggest it is prudent to review and prioritise the force records and systems that are vital to maintain policing services during and following an emergency with tolerable levels of risk to public safety and officer safety.

Next Steps – It is recommended the force keeps under review its vital records needs to be engaged in an emergency.

2.6.6 File structures

Current Situation – Consistent filing arrangements provide for the efficient sharing of records and are essential for ensuring information audit and assurance, and record keeping compliance. Currently our records are spread across several networks and multiple standalone IT systems with varying degrees of access. Within these systems there has been a tendency for teams (and individuals) to create their own record libraries resulting in an extremely complex, duplicative and expensive architecture that is poorly understood, brittle and vulnerable. This complexity has evolved over many years to resolve specific departmental needs rather than aligning with wider force needs. The result is that records needed by multiple users cannot be properly assessed and shared while they are in multiple versions held in multiple silos on multiple systems.

Next Steps - It is recommended the force improves its File Plan to structure its records holdings in a way that enables the linking of records across business areas to provide a single version of the facts.

2.7 Principle of Transparency

2.7.1 Retention and Disposal of Records

Current situation – The force follows national policing and departmental retention schedules to ensure our records are not retained longer than necessary, storage costs are minimised, and records worthy of preservation under the Public Records Act are identified at the earliest opportunity. The current issues impacting on our retention and disposal of records are;

(i) There are two Preservation Orders from the Independent Inquiry into Child Sexual Abuse (IICSA) and the Undercover Policing Inquiry (UCPI). The RRDU has identified and secured the relevant records for each and is ready to respond to requests from these Inquiries.

( )

.

(iv) While organisational records will be managed in accordance with JSP441 there is little guidance available to staff in an easily accessible format on how to manage the various policing records, other than nominal records on Unifi, throughout their lifecycle.

(v) Disposal arrangements detailing the correct procedures to follow when destroying records are contained in JSP440 to minimise the risk of an information security incident and ensure compliance throughout the record lifecycle. There has been little risk of a breach as very few records have been destroyed indicating there is a low level of awareness of procedures.

Next steps – To improve knowledge and change the culture on how policing records are managed throughout their lifecycle it is recommended the force produces a Record Review, Retention and Disposal Guidance and Schedule and makes this available on the force Intranet.

2.7.2 Archiving and Transfer Arrangements

Current situation - Clear arrangements for the transfer of material of enduring value to the RRDU and National Archives are needed to ensure that such records are identified and transferred at the earliest opportunity and the corporate memory of the force is fully and accurately preserved. Over the years there have been many internal records transfers to the force archives, however, these have taken place at irregular intervals and inconsistently, without any definitive guidance being followed.

Next steps - It is recommended a consistent set of transfer arrangements for both internal transfers and external deposits are produced to ensure consistency, streamline methods for transfer, define the

appropriate access status for various records, and identify any relevant legislative requirements. These arrangements should be in the form of an Archive Transfer Pack.

3. Records Management Improvement Plan

Principle	Recommendation
Accountability	
2.1.3 Governance	IAG and IXG review their terms of reference and re-commence regular meetings to complete the information governance arrangements
Competency	
2.2.1 Records Management Professionals	(a) RM to be identified as a distinct stream within the force training portfolio (b) Essential RM training and development to be identified in Role Profiles as part of comprehensive continual professional development process.
2.2.2 All Personnel	(a) Use Chronicle to record mandatory RM training (b) Force IM site collection on MODNet to provide one-stop shop for all RM needs and link to training
Compliance	
2.3.1 Legislation	Produce new Data Protection policy and guidance in an easily accessible format.
2.3.2 Standards	Engage with NPCC Data Quality portfolio and establish credible maturity matrix for RM to be used for internal assurance audits.
2.3.3 Force Policy and Procedure	Force policies and procedures for RM informally reviewed at least annually by FIM with a formal review alongside key stakeholders every 3 years.
2.3.4 Audit	Establish transparent RM audit process reporting to SIRO through Information Assurance Group.
Confidentiality	
2.4.1 GSC Marking	Compliance with GSC to be included as part of RM assurance process
2.4.2 Access Control	
2.4.3 Security Architecture	Security policies and procedures to be reviewed informally at least annually by ITSO with a formal review alongside key stakeholders every 3 years.
Integrity	
2.5.1 Audit Trail	Improve the management of electronic records by providing guidance to staff on use of metadata, document naming, and version control.

2.5.2 Data Quality	(a) Agree and apply consistent terminology for the creation of policing records, (b) Use MODNet migration as opportunity to cleanse records of duplicates and earlier versions
Availability	
2.6.1 ERDM systems	Project Board to be established for any new requirement for electronic record and document management systems.
2.6.2 E-Mail records	A consistent approach needs to be adopted to ensure relevant e-mail records are not lost
2.6.3 Criminal Justice System	Explore opportunities to reduce reliance on hard copy records and move to digital records wherever possible
2.6.4 Physical records	Review the management of unstructured records alongside continuing physical record needs and service provision with Project Jute in mind.
2.6.5 Vital Records	Review vital records needs that are to be engaged during and after an emergency.
2.6.6 File Structure	(a) Improve use of File Plan to structure our organisational record holdings (b) Use MODNet migration as opportunity to link records to provide a single version of the facts.
Transparency	
2.7.1 Retention and Disposal	Produce Record Review, Retention and Disposal Guidance and Schedule for policing records and make available on the force Intranet.
2.7.3 Archiving and Transfer	Produce consistent transfer arrangements for both internal transfer and external deposit to streamline methods for transfer, define appropriate access, and identify legislative requirements