Data Protection (Policy & Procedure)

OFFICIAL

Publication Scheme Y/N	Can be published on Force Website
Department of Origin	Corporate Support and Development Dept. (CSD)
Policy Holder	Head of CSD
Author	Data Protection Officer
Related Information	Computer Misuse Act Data Protection Act UK GDPR Government Security Classification Scheme Official Secrets Act Police and Criminal Evidence Act RRD Schedule APP Data Protection NPCC DP Manual of Guidance (log in required)
Date First Approved at BMG	25/1/2012
This Version	Version 2.0 - Amended 27/05/2022
Date of Next Review	29/06/2025 *(3 years from approval)*

May 2022

Contents

Version History

Version Number	Date	Rational behind amending/updating policy or procedure.	Policy Owner details
V.1.0	26/01/2012	First approved at Business Management Group 2501/2012	Head of PSD
V.2.0	27/05/2022	The policy was withdrawn in 2016 in favour of using content from APP. ICO audit in 2021 recommended a re-publication of a Data Protection Policy and Procedure to include local procedure guidance. Approved at SMB 29/06/2022	Head of CSD

Policy

Statement

Merseyside Police is committed to ensuring that all its officers, staff and agents undertake their legitimate duties in a manner compatible with data protection principles set out in the UK General Data Protection Regulations and the Data Protection Act 2018 (herein after described throughout this policy as 'the DPA 2018').

The Act regulates the use of information from which a living individual can be identified. It applies to the processing of personal data in most formats including electronic, paper and other media.

The Chief Officer lead for this policy is the Deputy Chief Constable whose role includes the Senior Information Risk Owner for the Force.

Aims

The main aim of this policy is to ensure that personal information is processed in compliance with the requirements of the Act and that all officers and staff are clear about what is regarded as acceptable or improper use.

The policy is underpinned by procedure that sets out required standards and details how those employees and any other authorised person having access to any force systems may process personal information lawfully and accountably.

Objectives

A broad objective is to process the personal data we have lawfully, fairly, and transparently. We must process personal data innovatively to maximise the opportunities derived from holding such data for the benefit of Force effectiveness and efficiency whilst safeguarding data subject rights. More specific associated objectives are to:

a) To be accountable for the ways personal data is processed.
b) Ensure all persons having access understand their responsibilities regarding their use of personal information.
c) Safeguard all personal data
d) Eradicate unlawful use of personal information
e) Protect the reputation of Merseyside Police by compliance with the legislation and NPCC Manual of Guidance.
f) Protect individuals from the use of inaccurate personal information, or misuse of accurate personal information.

Application and Scope

This policy provides a framework for ensuring that the Merseyside Police meets its obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 18). It applies to all the processing of personal data carried out by the Merseyside Police including processing carried out by joint controllers, contractors, and processors.
Merseyside Police complies with data protection legislation guided by the six data protection principles.
In summary, they require that personal data is:

- processed fairly, lawfully and in a transparent manner.
- used only for limited, specified stated purposes and not used or disclosed in any way incompatible with those purposes.

- adequate, relevant, and limited to what is necessary.
- accurate and, where necessary, up to date.
- not kept for longer than necessary; and
- kept safe and secure.

In addition, the accountability principle requires us to be able to evidence our compliance with the above six principles and make sure that we do not put individuals at risk because of processing their personal data. Failure to do so, can result in breach of legislation, reputational damage, or financial implications due to fines. To meet our obligations, we put in place appropriate and effective measures to make sure we comply with data protection law. Our staff have access to a number of policies, operational procedures and guidance to give them appropriate direction on the application of the data protection legislation, this includes:

This policy, which includes content about:

- Appropriate Policy documentation,
- Data Protection Impact Assessments,
- Protecting and responding to data subject rights,
- Records of processing Activities.
- Logging requirements

- ICT Acceptable Use Policy
- Information Risk Management Policy
- Information Security Policy
- Records Management Policy
- Review, Retention & Disposal Schedule
- Security & Personal Data Breach Policy

They are complemented by the Information Management Strategy.

This policy applies to persons at all levels of the organisation including all Police Officers, Police Staff, Special Constabulary, PCSOs, temporary staff, partner agency staff, consultants, contractors, and volunteers who have access personal data. They must be aware of, and are required to comply with, all relevant policy and associated procedures.

'Processing' of personal data means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. (Article 4.2 UKGDPR)

In plain terms 'processing' personal data means doing anything with it including looking at it (consultation).

Any processing of personal information that does not have a clear policing or other statutory or an identified business purpose is likely to constitute a misuse.

Merseyside Police will take criminal and/or disciplinary action against any category of person mentioned above who wilfully accesses and/or misuses personal information held by Merseyside Police.

Outcome Evaluation

The ways in which we process personal data will be subject to monitoring in several ways to assess how accountable we are for the way in which we process personal data and to maintain a high level of compliance with the legislation and to identify instances or processes which are not compliant, or which do not allow a demonstration of accountability. The ways in which this will be done are:

Regular activities

- Assurance Mapping
- Investigation of security or personal data breaches.
- Information Asset Owner monitoring of systems
- ICT activities
- Data Protection Impact Assessments
- Records of processing activities
- Logging Requirements
- Anti-Corruption Unit monitoring the use of personal information.
- PSD on associated issues.

Periodic activities

- Audits by Shared Internal Audit
- CSD Analysis and Evaluation

Procedure

1. Overview

1.1 Authorised Professional Practice (APP) is produced by the College of Policing as the official source of professional practice on policing. All officers and staff are expected to have regard to APP in discharging their responsibilities. Essentially, our "policy" is to comply with APP as it develops to cover all areas of policing.

1.2 Where content exists within APP, we should not be reproducing it locally but instead signposting the on-line version. Similarly, we should not retain or develop any local policy documents if the subject matter is covered by APP. We may have some relatively low volume procedural documents but only if they are deemed necessary to supplement the content of APP.

1.3 In addition to APP there is the Police Knowledge Hub which provides information and a portal to share current thinking around an expanse of policing subjects.

1.4 The NPCC Data Protection Manual of Guidance (MOG) is available via the Knowledge Hub but it is also available on this iForce page Information Assurance and Data Protection (sharepoint.com) It is intended for data protection practitioners but may be of assistance to other users. It is advised that if general users need to consult this guidance, which is a comprehensive and in-depth document, then the Information Assurance Team (DPO, IAC or Information Compliance Officers) should be consulted prior to doing so.

1.5 This procedure will therefore contain local procedures which are not available on APP

2. Roles & Responsibilities

2.1 **Internal Structure**
This section describes the internal structure for Information assurance within Merseyside Police.

2.2 **The Data Controller**
is the Chief Constable and is ultimately accountable for the information and personal data processed by the Force.

2.3 **The Senior Information Risk Owner (SIRO)**
is the Deputy Chief Constable of Merseyside Police, who holds the delegated responsibility for oversight of this policy. The SIRO leads and fosters a culture that values, protects and uses information for the public good. The SIRO will manage information risks alongside financial, legal and operational risks which are also faced by the Force. These are considered in terms of the Force's strategic business and operational objectives and how they may be impacted by the failure of information systems. The SIRO is accountable to the Chief Constable.

2.4 **The Head of Strategy and Business Development**
Part of the remit of this role is to provide the force with the underpinning risk management processes necessary to drive effective and efficient strategic decision making. This includes the coordination, maintenance and promotion of risk management arrangements within the Force in line with the principles of risk management. The post holder will report to Chief Officers on the risk profile at regular intervals via the corporate meeting structures.

2.5 **The Information Asset Owners (IAOs)**
are senior individuals involved in the running of specific business areas. Their role is to understand what information is held, what is added and what is removed, how information is processed and who has access to it and why. As a result, they are able to understand and address risks to the information and ensure that information is fully used within the law for public good. They will receive bespoke training and refresher training in the role. IAOs will submit annual scheduled reports to the SIRO Board in respects of their assets and additional reports when 'triggered' by any events in the interim period. This will be reflected in the SIRO Board Terms of Reference. Merseyside Police should continue with their work in expanding a privacy culture across the Force through their network of IAOs. using their IAOs as communication channels from senior management to provide key messages about DP, RM and IS. They should ensure that they have processes to implement appropriate organisational and technical measures to comply with DP principles, when determining the means of processing and review them regularly to ensure they remain effective and appropriate throughout the processing.

2.6 **The Data Protection officer (DPO)**
provides professional advice and guidance to the organisation on compliance with the Data Protection Act 2018 (DPA) and UK GDPR, informing and advising the data controller, the SIRO and other roles of the force's obligations under the DPA and monitoring compliance by all roles. The DPO will be involved in the development and monitoring of all DP related policies and procedures

2.6.1 The designation, position and tasks of the Data Protection Officer are defined in sections 69-71 of the DPA 2018 and is a statutory role.

2.6.2 The role must be entrusted with the following tasks:

- providing advice on the carrying out of a data protection impact assessment under section 64 and monitoring compliance with that section,

- co-operating with the Information Commissioner, acting as the contact point for the Commissioner on issues relating to processing, including in relation to the consultation mentioned in section 65, DPA 2018 and consulting with the Commissioner, where appropriate, in relation to any other matter including ensuring the annual notification with the ICO.

- In relation to the policies concerning data protection, the Data Protection Officers' tasks include—
- assigning responsibilities under those policies,
- raising awareness of those policies,
- training staff involved in processing operations, and
- conducting audits required under those policies.

- In performing the tasks set out above, the data protection officer must have regard to the risks associated with processing operations, taking into account the nature, scope, context and purposes of processing.

- This role has additional responsibilities as described in part 14 of this procedure.

2.7 **The Information Assurance Coordinator (IAC)**
coordinates, develops and implements information assurance initiatives to meet the force's statutory responsibilities and ensure compliance with the police Community Security Policy, current legislation and all national/local, Home Office, College of Policing and NPCC policy objectives. The IAC will monitor the Force's information security controls. This role has additional responsibilities as described in part 14 of this procedure.

2.8 **The Information Compliance Officers**
conduct monitoring and compliance activities under the direction of the IAC with DPO advice. They will use a variety of methods including assurance mapping, recording and initial investigation of security or personal data breaches, assistance with completion of records of processing activities and logging requirements, monitoring reviews of policy and other reviewable documents and ancillary duties to improve compliance with information security/assurance.

2.9 **The Information Technology Security Officer (ITSO)**
develops and implements IT Security policy and procedures, with specific responsibility for IT and communications systems security. The ITSO provides technical advice and ensures information risks are brought to the attention of the IAO and/or specialists within the Information Management business area during any new system design, development or configuration that might affect the confidentiality, integrity, or availability of force information. The ITSO is the first point of contact for the DPO in respect of data protection matters and the ICT Department. The ITSO will be involved in the development of IT security policies in liaison with the IAC and/or DPO. They should ensure that they have processes to implement appropriate organisational and technical measures to comply with DP principles, when determining the means of processing and review them regularly to ensure they remain effective and appropriate throughout the processing.

2.10 **The Force Records Manager**
ensures availability, integrity and confidentiality of personal data and other records and its' timely review, retention, or deletion. The role also ensures that records are held in accordance with the data protection principles as summarised in the application and scope part of the policy above.

2.11 **The Professional Standards Department (PSD)**
and the Anti-Corruption Unit (ACU) are responsible for auditing and investigating all instances of information systems and related equipment and information misuse.

2.12 **Line Managers and Supervisors**
have an important role to play and are responsible for ensuring that all members of staff under their responsibility comply with the standards set out in this Policy and its supporting policies and procedures. They must monitor the processing of personal data by those under their supervision and bring to the attention of the DPO any training gaps or requirement they may discover.

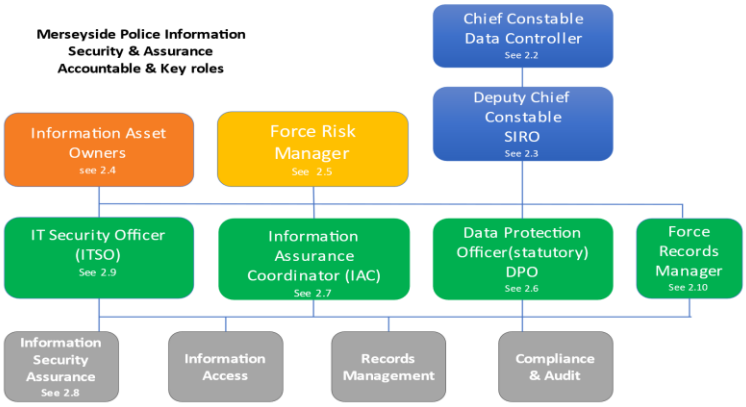
2.13 **All information users**
with access to Merseyside Police's assets have a responsibility for safeguarding those assets. Every individual must be aware of relevant policies and procedures and ensure that they have permission and authority to access data and systems on a legitimate operational need to know basis. Users are encouraged to bring to the attention of their Line Manager any events of any weaknesses in security arrangements and report all suspected security incidents following the Security Incident Reporting Procedure.

2.14 **Practical documentary guidance**
will be provided to all of the above roles and operational staff as required in respect of this policy. This guidance will be made available and communicated to staff and should be subject to regular review. See Training and Guidance at part 6 of this procedure.

3. Control and Governance

3.1 Some of the roles mentioned above form part of the Information Management Structure. They meet approximately quarterly at the Senior Information Risk Owners' (SIRO) Board where matters of information management, risk and assurance are subject of strategic consideration and decision making. An organisation chart depicting

this is below. The SIRO Board has a written term of reference (reviewable). It will maintain standing attendees and agenda items which includes reporting from all key IG functions, including the DPO, RM and IS. The reporting should include KPIs, issues and risks.



3.2 Under the oversight of all IAOs, Operational level meetings that are minuted and have an action plan in place. The agendas should allow for appropriate DP matters to be discussed and the outputs from those meetings should feed into the SIRO Board. Ground level staff should be able to raise DP and IS matters to these groups. This will help MP gain assurance that there is coordination for DP and IG activities across the Force. These groups should act as a channel for communication of information and risks to the SIRO Board.

3.3 A flowchart depicting the Information Governance and Compliance Cycle is at part 11.1 of this procedure.

4. Supporting and Associated Policies and Procedures

4.1 This policy does not stand alone as the sole source to address information governance, risk, compliance, and security within Merseyside Police. The other policies listed (alphabetically) below provide information and local procedure about other aspects of how Merseyside Police will approach all facets of information governance. All of these polices must be read upon induction except those at parts 4.5 and 4.12. Those involved in ICT or vetting business areas must also read these policies and procedures. The Information Assurance team will monitor compliance with this.

4.2 **Data Protection Policy.** (This policy) Ensures that personal information is lawfully and appropriately processed by the Force in compliance with the requirements of the Data Protection Act and UK GDPR and that all officers and staff are clear about what is regarded as acceptable or improper use. Link to policy page

4.3 **Government Security Classification Scheme.** Assists all personnel to understand and use Security Classifications in accordance with national police guidance to adequately protect information and personal data. Link to policy page

4.4 **ICT Acceptable Use Policy.** Safeguards the confidentiality, integrity and availability of force information by clearly setting out expectations regarding acceptable use of ICT systems and the devices used to get access to those systems. Link to policy page

4.5 **ICT Compliance Policy & Procedure.** Sets out the Force's approach to DP, IS governance and practice in an IT setting ensuring that the DPO, ITSO and IAC are

involved in the development of information security policies. It includes the appropriate identification and classification for all electronic records to ensure documents are appropriately protected and sharing is restricted in line with the classification requirements by assigning, and documenting access levels and controls based on the principle of least privilege, in line with an individuals' role. This is to minimise the risk that users may have access to information which should be restricted from them by monitoring amending and revoking access in a timely manner.
Innovate and document how staff should handle the transfer of all electronic personal data internally and externally, providing relevant training as required to maintain the confidentiality, integrity and availability of personal data processed. Document process for handling and storing IT equipment used to process personal data prior to destruction to minimise the risk of a PDB. Link to policy page

4.6 **Information Risk Management Policy.** Sets out the organisational structure, policies and procedures that are in place to manage information risks. Facilitates effective clear direction and supports achievement of compliance with legislation, statutory obligations and good practice standards. Link to policy page

4.7 **Information Security Policy.** Sets out policy and procedure to ensure safeguards, measures and countermeasures are put in place to provide the continued confidentiality, integrity, availability and validity of Force information and information systems to a standard of non-repudiation. Link to policy page

4.8 **Physical Security Procedure.** Provides details on how to protect physical assets including property, employees and the information that Merseyside Police holds and accesses.

4.9 **Protective Monitoring Procedures.** Defines the monitoring and auditing of staff activity as a means of ensuring all staff comply with Force policy and procedures and with the standards of behaviour expected by Merseyside Police. This is an OFFICIAL-Sensitive document with limited role related access control.

4.10 **Records Management Policy and Review, Retention & Disposal (RRD) Schedule.** Provides guidance on lawful processing of electronic, paper, and other media-based information and personal data deployed in the Force. Link to policy page Link to RRD schedule

4.11 **Security and Personal Data Breach Notification Policy.** Provides guidance on the processes and procedures for managing security incidents including the reporting of security breaches Link to policy page

4.12 **Vetting Policy.** Ensures that all staff employed by Merseyside Police and our service providers are honest and act with the highest integrity through conducting vetting checks on all our staff (including volunteers) which are proportionate and appropriate to their role. Link to policy page

4.13 The table below will direct users to the relevant policy for additional guidance about specified subject matters which might otherwise have been included in this Data Protection Policy & Procedure. These subject areas are as recommended by the ICO to achieve improved compliance. The policies can be found in the iForce policies section alphabetically by the title of it. Link to policy page

Key
1 – Security and Personal Data Breach P&P
2 – ICT Acceptable Use P&P
3 – ICT Compliance P&P
4 – Information Management Strategy
5 – Information Risk Management P&P
6 – Information Security P&P
7 – Records Management P&P

DP requirement	1	2	3	4	5	6	7
Put in place detailed procedures for creating records or developing documented information across the organisation. Procedures should be created with input from the Records Manager and include naming conventions to ensure consistency and make it easy for staff to identify correct versions of documents.				X			X
Ensure that procedures and checks are in place across the organisation to have the appropriate identification and classification for all records/information (manual and electronic). This will also ensure documents are appropriately protected and sharing is restricted in line with the classification requirements of OFFICIAL or OFFICIAL-sensitive, etc.			X	X		X	X
Assign, and document access levels and controls based on the principle of least privilege, in line with an individuals' role and who accesses personal data (manual and electronic) to ensure that appropriate access levels are implemented when any records or information is created and minimise the risk that users may have access to information which should be restricted to only those who have a justifiable business purpose for doing so. They should be reviewed regularly and included in formal auditing processes.		X	X	X		X	X
Formal detailed process(es) of how access to electronic records on all systems is to be granted, monitored, and amended/revoked.			X	X		X	X
Ensuring that all systems used for processing personal data have the correct access controls applied which access is regularly reviewed and monitored to preserve the integrity and security of the personal data as required under the logging purposes in s.62(4) DPA18.			X				
Identify all records that have not been returned to the RM store and trace them to ensure they can be accounted for or logged as a breach incident if necessary. Document the procedure for the removal of any manual and audio/ visual records that contain personal data and put in place controls for the safe storage and use of the record once signed out. The process needs to include a follow up process for files not returned within a set period/date ensuring accurate tracking of manual records to identify and report breaches as appropriate.						X	X
MP should put in place procedures which clearly set out the process for indexing, retrieving and tracking records stored in archive facilities to include statutory timescales to adhere to and be communicated and readily available for all staff.							X
Conduct compliance checks to measure the effectiveness of the retrieval and tracking systems and identify security or data breaches. Create KPIs to measure the performance for record retrieval to feedback to the SIRO Board to document any actions required.							X
Establish a programme of regular data quality checks that include all systems that process personal data and manual records to include confirmation that information continues to be adequate for its original purposes. Records of these checks should be maintained, and the results of data quality reviews should be acted on to refresh and improve							X

information retention practices to comply with Article 5(1)(c) UK GDPR and s.37 DPA18.							
Develop and document a process to provide the results of data quality audits and spot checks to staff across all systems and manual records containing personal data to gain assurance that staff are aware of existing issues and are able to act to improve practices.				X			
Ensure that personal data stored on all forms of removable media is made secure with appropriate encryption, this will help to preserve the confidentiality, integrity, and availability of the personal data. The process should be documented and communicated to all staff.			X				X
Document how staff should handle the transfer of all personal data (manual and electronic) externally by any means including but not limited to post, collection from premises and email. Training should be given communicating the procedure to all staff to utilise the guidance, accessible on iForce to ensure the confidentiality, integrity and availability of personal data.			X			X	X
Periodically weed all information systems and manual records (active and archived) forming part of a continuous programme documented in a policy and procedure in accordance with the retention schedule. Implement automatic weeding (where appropriate and possible) for electronic records.							X
Review their retention schedule as part of their data mapping exercise, to ensure that the Information Asset Register/ROPA and retention schedule mirror one another. Any further processing activities identified which are not reflected within the NPCC guidance, should be assigned a retention period and formally documented.							X
A programme of regular reviews should be conducted and documented to ensure that the retention schedule meets all the necessary requirements and does not result in information being retained past the point of necessity.							X
Oversight of retention and disposal for all records on all systems (both electronic and manual) is to be assigned to an appropriate person (such as IAOs). The assigned person should receive RM training and any changes made to the retention schedule should be approved and a history of changes retained. **This responsibility lies with the Force Records Manager.**							X
Ensure all electronic records that are MOPI 2 are reviewed and assessed to ensure they remain appropriate to be retained or disposed of accordingly.							X
Review and document their process for handling and storing IT equipment used to process personal data prior to destruction to minimise the risk of a PDB.			X				
MP should continue to work through the backlog of MOPI 2 graded files and extend that work into MOPI 3 graded files to minimise the risk of personal data being retained for longer than is necessary. MP should also ensure that the risk of over retention for the MOPI 2 and MOPI graded records is recorded on the information risk register. Ensure that retention periods are set for all manual records. In addition, put in place procedures so that when electronic							X

records are deleted that any corresponding physical hard copy file or evidence is also disposed of.							
Document and review the process for handling and storing confidential waste prior to destruction and ensure there are appropriate security controls in place to minimise the risk of a PDB whilst those records are being stored prior to destruction.						X	X
Ensure that manual records awaiting destruction are stored in a limited access secure area to assure that personal data contained within manual records is not at risk of a breach whilst the records are stored prior to destruction.							X
Introduce breach notification policy with detailed guidance. Develop comprehensive guidance for staff responsible for breach management and incident response to follow in the event of a security incident. This should include the procedure for managing and recording near-misses. Provide guidance or links on their Information Assurance page to enable staff to readily access policies and guidance.	X		X			X	
Ensure that all staff who handle personal data are able to recognise and report a PDB. A TNA should be undertaken for all staff and where a need is identified, appropriate level of training and support should be provided on how to recognise and report a PDB. The training should cover PDB scenarios which may occur in MP as well as the incident reporting process. The training should be regularly refreshed.	X					X	
Ensure that specialist training is provided and regularly reviewed and refreshed for PDB decision makers to follow when managing and responding to a security incident to combine procedures with legislative requirements. This will ensure that senior staff have received appropriate training to allow them to assess the severity of a PDB and formulate a response.						X	
Review any sharing of personal information they do with third party organisations, to identify any data controllers they jointly process data with. Where joint controller arrangements apply, ensure there are agreed communication channels and procedures between parties in the event of a PDB, including nominated points of contact. This should be detailed in contracts and agreements in compliance with Article 26 UK GDPR.						X	
Review all contracts with data processors to ensure they adequately reflect the processor's obligations in the event of a PDB. The review should ensure that contracts include agreed channels of communications or nominated persons and a time scale to report PDBs. Have processes, such as planned visits or audits to gain assurance that the data processors are clear in their obligations to inform MP if a PDB has occurred as well as being able to detect or find PDBs within their systems and processes. Ensure that there is clear oversight of their data processors, have laid out their expectations in a written contract and have a procedure in place to fulfil the contract in the event of a breach.						X	

Procedures and guidance in place to ensure staff are able to identify and follow the process to report a PDB within the required timeframe as required by the legislation. Put in place targeted training or awareness campaigns at regular intervals to ensure staff are confident at recognising a PDB and reporting them. Introduce measures to ensure that incidents uncovered by PSD and ACU are reported to Information Assurance without delay when an issue is uncovered.	X					X	
Have means to assess the severity of PDBs by: i. continuing their work with their ROPA to ensure that all information processed is documented, including the categories of personal data and the security measures in place. ii. documenting the set criteria for assessing the severity of the breach and the likely effect on individual's rights and freedoms. This guidance should reference risk assessment guidance, such as the ICOs PDB criteria (likelihood and severity) and should provide particular guidance over how to assess a 'high risk' to affected individuals. iii. The categories of personal data should be included in the security breach form and be proactively risk assessed to determine the possible level of risk to an individual should a PDB occur. When risks are identified, they should be added to an appropriate risk register and/or any DPIA that has been carried out. In compliance with s.67 DPA18.	X						
Periodically review their Security Breach Form to include the requirement to assess and record the possible impacts of the incident on the rights and freedoms of the individual in compliance with s.67(6) DPA18. (C.09(a)) Define and document near miss incidents. Have documented guidance for staff who record and assess PDBs to include the requirement to log near-miss incidents to understand the risks associated with its processing and identifying mitigating actions before a PDB occurs.	X					X	
Have a procedure for the identification, logging, management, assessment and reporting of PDBs that occur 'out of hours', when a decision maker is absent and if a communication channel has been compromised by a breach. This to be made available to all staff with responsibility for assessing PDBs and reviewed regularly. PDBs should be reported to the ICO within 72 hours of becoming aware of the breach, unless they are unlikely to cause a risk to the rights and freedoms of individuals. MP should develop guidance for staff to follow when reporting PDBs to the ICO. The ICO should be notified of a PDB if there is a risk to the likelihood and freedoms of individuals. Identify and document its lead supervisory authority where there is a potential for a cross border breach. This should form part of the breach response plan.	X					X	

In compliance with Article 34 UK GDPR and s.67 DPA18.							
Have available guidance to follow when identifying root causes of PDBs. This should include: i. the Breach Security Form should be a live document and be updated with any essential information from additional correspondence. ii. the requirement to report any identified risks to senior management for inclusion on a relevant risk register. ii. a process to periodically review risks from previous breaches. In compliance with Article 5(1)(f) UK GDPR and s.34(1)(f) DPA18.	X					X	

5. General Obligations (and required activities)

5.1 The College of Policing APP website contains information about data protection and UKGDPR via this Data Protection at APP

5.2 The obligations from the legislation covered in this procedure are detailed in the table below. It lists the obligation, a brief description of it and the main accountable roles are in the table. They refer to documents that we must have and maintain by regular review or actions that we must take at required intervals or when triggered by events.

Obligation	Description	Accountable Roles
Appropriate Policy documentation S42 DPA 2018 (Subject to regular review)	Outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category (SC) and criminal offence (CO) data under certain specified conditions. ICO guide re APD S42 DPA 2018 APD	Data Protection Officer
Protecting and responding to data subject rights Part 3 Chapter 3, Ss 43 -54 DPA 2018 (Triggered by requests)	Data protection law aims to empower individuals and give them greater control over their personal data through several rights, which you need to facilitate effectively. Compliance with individual rights minimises the privacy risks to individuals as well as to organisations. ICO guide to Individuals rights S43 DPA 2018	Data Access Analyst for subject access requests. Data Protection Officer for all other data subject rights.
Overview and scope **for law enforcement purposes.**	S31 DPA 2018 Law Enforcement Purposes S55 DPA 2018	All

S55 DPA 2018		
General obligations of the controller S56 DPA 2018	ICO guide to Controllers & Processors S56 DPA 2018	All
Data protection by design and default S57 DPA 2018 (Triggered by change)	ICO guide to DP by design & default S57 DPA 2018 A 'DP by design and default' approach must be taken. This includes only processing personal data which is necessary for each specific purpose of processing. This is reflected in the DPIA guidance. It is to be implemented when conducting data mapping for all existing processing activities. The Records Manager should ensure that retained data is reviewed on a regular basis to identify opportunities for pseudonymisation and/or minimisation and this is documented in the retention schedule.	All involved in new projects, processes and innovation and thereafter on a review basis.
Joint controllers S58 DPA 2018 (Triggered by change)	ICO guide to Joint Controllers S58 DPA 2018	Data Controller Data Protection Officer IAOs
Processors S59 DPA 2018 (Triggered by change)	ICO guide to controllers & processors S59 DPA 2018	Data Protection Officer IAOs Information Assurance Coordinator Information Compliance Officers Processors of personal data on behalf of the data controller
Processing under the authority of the controller or processor S60 DPA 2018 (Triggered by change)	ICO guide to data processors S60 DPA 2018	Data Protection Officer IAOs Information Assurance Coordinator Information Compliance Officers Processors of personal data on behalf of the data controller
Records of processing Activities S61 DPA 2018	ICO guide to ROPAs S61 DPA 2018	Data Protection Officer Information Compliance Officers

(Triggered by change)		All involved in completing the ROPA document.
Logging requirements Rights of the data subject S62 DPA 2018 (Triggered by change)	ICO guide to Logging S62 DPA 2018	Data Protection Officer Information Compliance Officers All involved in completing the ROPA document.
Co-operation with the Commissioner S63 DPA 2018 (Triggered by requests)	Each controller and each processor must co-operate, on request, with the Commissioner in the performance of the Commissioner's tasks.	Data Protection Officer
Data Protection Impact Assessments S64 DPA 2018 (Triggered by change)	ICO guide to DPIAs S64 DPA 2018 The requirements of the DPIA is covered in depth within the Information Risk Management Policy and procedure and at part 11.5 of this procedure and is fully explained within the guidance present in the DPIA template which is available in this iForce page Information Assurance and Data Protection (sharepoint.com)	Data Protection Officer Information Assurance Coordinator Information Compliance Officers Any involved in new projects or processes and reviewing existing ones.
Prior consultation with the Commissioner S65 DPA 2018 (Triggered by change)	S65 DPA 2018	Data Protection Officer as Force SPOC with ICO.
Security of processing S66 DPA 2018 (Triggered by change)	ICO guide to security outcomes S66 DPA 2018	Data Protection Officer Information Assurance Coordinator Information Compliance Officers
Notification of a personal data breach to the Commissioner S67 DPA 2018 (Triggered by events)	ICO guide to personal data breaches S67 DPA 2018	Data Protection Officer as Force SPOC with ICO.
Communication of a personal data	If a breach is likely to result in a high risk to the rights and freedoms of individuals, the	Data Protection Officer Information Compliance Officers

breach to the data subject S68 DPA 2018 (Triggered by events)	UK GDPR says you must inform those concerned directly and without undue delay. ICO guide on informing data subjects of a breach S68 DPA 2018	

Here are some links to APP
APP Data Protection
APP Information Sharing
APP Information Management

6. Definitions

6.1 Personal Data – means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; (UKGDPR Article 4.1)

S.3(2) of the DPA 2018 further defines personal data as any information relating to an identified or identifiable living individual.
S.3(3) defines "Identifiable living individual" means a living individual who can be identified, directly or indirectly, particularly by reference to—
(a) an identifier such as a name, an identification number, location data or an online identifier, or
(b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of the individual.

6.2 "Processing", in relation to information, means an operation or set of operations which is performed on information, or on sets of information, such as—
(a) collection, recording, organisation, structuring or storage,
(b) adaptation or alteration,
(c) retrieval, consultation, or use,
(d) disclosure by transmission, dissemination or otherwise making available,
(e) alignment or combination, or
(f) restriction, erasure, or destruction,

6.3 "Data subject" means the identified or identifiable living individual to whom personal data relates.

6.4 "Material Scope" UKGDPR article 2 describes what personal data the Regulation applies to and what personal data is not applicable.

6.4.1 What personal data is applicable?
Personal data processed by automated means (electronic system/computer)
Other processing by paper/hardcopy or other media forming part or is intended to form part of a filing system.

Merseyside Police is also subject to the Freedom of Information Act 2000 (FOI) so manual unstructured data is also subject to UKGDPR so far as responding to FOI requests is concerned.

6.4.2 What personal data is not applicable?

- *The processing of personal data by an individual in the course of a purely personal or household activity.* This means that UKGDPR does not apply to private citizens when conducting their own domestic matters. It does **not** mean that persons having access to personal data on police systems can process that personal data for their own private purposes.

- *The processing of personal data by a competent authority for any of the law enforcement purposes (see Part 3 of the 2018 Act);* This makes it clear that when processing for law enforcement purposes the DPA 2018 Part 3 is the primary legislation to follow.

6.4.3 The text of UKGDPR refers to an 'IP Completion Day' It means 'Implementation Period' completion day, the ending of the 11-month period from 31 January 2020 during which the UK continued to be subject to EU rules. It was 31/12/2020 and was known as the transition period to the UK leaving the EU.

6.4 Further definitions are at article 4 of UKGDPR and Ss 3 to 7 of the DPA 2018.

7. Purpose

7.1 The principal purpose for which Merseyside Police processes information is a 'Policing Purpose'. This is defined as:

a) Protecting life and property
b) Preserving order
c) Preventing the commission of offences
d) Bringing offenders to justice
e) Any duty or responsibility arising from statute or common law.

Information is also processed for specific purposes connected with the administration of the Force and its employees.

7.2 The Force could not exist and cannot function without 'processing' personal data. We process personal data for two main purposes so far as the legislation is concerned. They are for 'general' purposes and for 'law enforcement' purposes.

7.3 Law Enforcement purposes are defined at S31 of the DPA 2018 as the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. The requirements for law enforcement processing are found within part 3 of the DPA 2018.

7.4 General purposes are any purpose which is not a law enforcement purpose defined above. The requirements for general processing are found within part 2 of the DPA 2018 which repeatedly refers back to the UKGDPR.

7.5 The two purposes above must be 'direct' purposes. It must not be assumed that because we are a police force then the ultimate aim is to enforce the law, so all processing is for a wider law enforcement purpose. For example, recruiting a police officer is not a law enforcement purpose, it is a general purpose.

7.6 For the avoidance of doubt, even though a police force collects intelligence, it is not an 'Intelligence service' as defined in the Act so the rules in part 4 of the DPA 2018 do not apply to police forces.

7.7 The DPA 2018 cannot be read in isolation from the UKGDPR because the DPA 2018 repeatedly refers back to the UKGDPR.

8. Conditions for Processing

8.1 At the outset of processing personal data it must be decided which of the two purposes applies because the rules for compliance are different in either case.

8.2 The first data protection principle at article 5 of UKGDPR is that Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. The first data protection principle under S35 of DPA is that the processing of personal data for any of the law enforcement purposes must be lawful and fair. The requirement for transparency is not present for law enforcement purposes due the detrimental effect that transparency with data subjects may have on investigations and other law enforcement purposes.

8.3 When it has been identified whether processing of personal data is for a general purpose or a law enforcement purpose it must be further identified whether the personal data is simple personal data or whether it includes special categories of personal data and/or criminal conviction and offence personal data as part of the processing. The document called the **Record of Processing Activity** (ROPA) is a template that must be completed for each process to comply with S61 of the Act so that Merseyside Police can demonstrate compliance and achieve accountability. It is also a useful way of navigating through the process to ensure that what you intend to do, or are already doing for existing processing, is lawful, fair and when required transparent. Completion of the ROPA is required only once for any process but needs to be reviewed/completed again when an existing process changes. The ROPA is available on iForce via this link Information Assurance and Data Protection (sharepoint.com)

8.4 It will be seen that whether processing personal data for a general purpose or a law enforcement and whether personal data or special category personal data or sensitive personal data for law enforcement purposes is to be processed, an abiding available condition is that of consent or explicit consent. There are other more appropriate conditions other than consent and whenever applicable they should be relied upon. A difficulty with relying upon consent is that it may be withdrawn at any time by the data subject. In such an event, processing must then cease and other parties with which that personal data has been sent must be informed that consent no longer exists. The ICO provides significant guidance on many aspects of consent which may be accessed via this ICO re consent link. In addition a specific guide about local procedure for consent will be available on this iForce page Information Assurance and Data Protection (sharepoint.com)

9. Processing for a general purpose

9.1 For processing of personal data to be lawful it must meet a condition of article 6 of the UKGDPR. Much of the processing of personal data carried out by a public authority is carried out under article 6(1)(e) namely the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. This is often referred to as 'a public task'. The DPA 2018 at S8 defines what the public interest means. It reads:

9.2 In Article 6(1) of the GDPR UK GDPR (lawfulness of processing), the reference in point (e) to processing of personal data that is necessary for the performance of a task carried out in the public interest or in the exercise of the controller's official authority is defined by S8 of the DPA 2018 as processing of personal data that is necessary for—
(a) the administration of justice,
(b) the exercise of a function of either House of Parliament,
(c) the exercise of a function conferred on a person by an enactment or rule of law,
(d) the exercise of a function of the Crown, a Minister of the Crown, or a government department, or
(e) an activity that supports or promotes democratic engagement.

Please refer to the ROPA document mentioned in 8.3 above to assist in navigating through to identify lawful processing and thereby accounting for the processing of personal data.

9.3 Personal data is defined at 6.1 above

9.4 Special categories of personal data is defined in UKGDPR article 9.1 as:
Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

9.5 It is apparent that the default position is that special categories of personal data cannot be processed unless a condition in article 9.2 is identified. Some of the conditions do not apply to a police force. The relevant conditions are summarised as:

- With explicit consent of the data subject. – this should ideally be written/recorded and not merely verbal.
- necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law.
- necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent. – 'Vital' means life threatening situations, not merely important to achieve an aim.
- relates to personal data which are manifestly made public by the data subject.
- necessary for the establishment, exercise, or defence of legal claims or whenever courts are acting in their judicial capacity
- processing is necessary for reasons of substantial public interest, on the basis of domestic law.
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of domestic law. – this would cover OHU activities
- processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law domestic law which provides for suitable and specific measures to safeguard

the rights and freedoms of the data subject, in particular professional secrecy domestic law. – this condition was not considered relevant to the activity of a police force but was unusually used during the Covid pandemic.

- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) [(as supplemented by section 19 of the 2018 Act)] based on domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject

The conditions should be read in full when considering whether they are applicable to the processing under assessment

9.6 The DPA 2018 at S10 imposes additionally conditions to those contained in UKGDPR Article 9.2 (as summarised at 9.5 above). They involve identifying a further condition within specified schedules of the DPA 2018. To explain this, the table below provides guidance on which schedules need to be viewed and a relevant lawful condition identified based upon the condition within article 9.2 on which reliance is placed for lawful processing. **Using the ROPA document will assist, using tabs 5 and 5A.**

Conditions in article 9.2 of UKGDPR	**DPA Schedule condition to be identified**
(a) Explicit consent	No condition required
(b) (employment, social security and social protection);	Schedule 1 Part 1
(c) Vital interests	No condition required
(d) Not a relevant condition	No condition required
(e) data made public by the data subject	No condition required
(f) the establishment, exercise or defence of legal claims	No condition required
(g) (substantial public interest);	Schedule 1 Part 2
(h) (health and social care);	Schedule 1 Part 1*
(i) (public health);	Schedule 1 Part 1
(j) (archiving, research and statistics).	Schedule 1 Part 1

* When personal data is processed under article 9.2(h) then those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under domestic law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under domestic law or rules established by national competent bodies. For Merseyside Police that refers to a doctor (OHU) or other medical practitioner who is subject to the same obligation of secrecy by their profession or under the supervision of such a role.

9.7 In the previous Data Protection Act 1998 personal data relating to criminal conviction and offences was included in the definition of ‘sensitive’ personal data along with most of the other categories of personal data now defined as special category personal data in the UKGDPR. The UKGDPR addresses processing of personal data relating to criminal convictions and offences separately in article 10. This is because the conditions for processing conditions for processing criminal conviction and offence data are different from the conditions in article 9.2 as summarised in 9.5 above.

9.8 Section 11(2) DPA 2018 clarifies that references in S10 to criminal convictions and offences or related security measure include personal data relating to the alleged commission of offences by the data subject, or proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing.

9.9 Processing personal data concerning criminal conviction and offences clearly takes place for law enforcement purposes but there are also many reasons to process personal data of these categories for general purposes too. Vetting, HR and responding to regulatory bodies are examples of such processing for general purposes.

9.10 There are three conditions imposed by article 10 of the UKGDPR to lawfully process personal data concerning criminal convictions and offence or related security measures. They are:

- Processing is carried out under the control of official authority – 'official authority' is termed as 'competent authority' in the DPA 2018, and they are listed in schedule 7 of the Act. Merseyside Police is a competent authority as mentioned at 7.5 of the Schedule as are other police forces

- A Competent Authority is defined at S30 of the DPA 2018 as a person specified or described in Schedule 7, and any other person if and to the extent that the person has statutory functions for any of the law enforcement purposes. This leaves scope for persons not mentioned in schedule 7 to be treated as a competent authority of they have statutory law enforcement functions as defined in S31 of the Act.

- Processing is authorised by domestic law – Authorities or organisations which are not listed as competent authorities in DPA 2018 Sch 7 must have a basis in law to lawfully process conviction or offence personal data. In addition, when processing special category or criminal conviction or offence personal data, an organisation must meet a condition of Schedule 1 in Parts 1, 2 or 3 per S10(5) of the DPA 2018. Although this condition does not apply to Merseyside Police it is if value to know when processing such personal data to bodies which are not competent authorities.

- Any comprehensive register of criminal convictions shall be kept only under the control of official authority – only an organisation listed in schedule 7 may keep such records, e.g., PNC or other internal systems such as Niche and Corvus

9.11 Because of the conditions for processing personal data concerning criminal convictions and offences described at 9.10 above, it is important to establish whether a body is a competent authority or not because the conditions for disclosing/sharing criminal conviction or offence personal data and other personal data are different. There are 56 bodies or types of bodies in DPA 2018 schedule 7 which are categorized as follows:

- Any United Kingdom [ministerial] government department
- Chief officers of police and other policing bodies
- Other authorities with investigatory functions
- Authorities with functions relating to offender management
- Other authorities

9.12 Competent Authorities which are of relevance to Merseyside Police processing of personal data are mentioned alphabetically below. The number alongside is the entry in schedule 7. Some relate only to specified functions so the schedule should be consulted to reach a decision about processing of personal data:

- Border Revenue – 26
- Court or Tribunal – 56
- Criminal Cases Review Commission – 34
- Director of Public Prosecutions – 47
- Electronic monitoring of individuals - 45
- Financial Conduct Authority – 27
- Health & Safety Executive – 28
- HM Land Registry – 33

- HM Revenue & Customs – 21
- Independent Office for Police Conduct – 18
- Information Commissioner – 52
- National Crime Agency – 24
- Parole Board for England and Wales – 38
- Prison, Young Offending Institutes or Secure training – 43
- Prison escorts under contract – 44
- Probation Services – 36
- Serious Fraud Office – 25
- Youth Justice Board for England and Wales – 37
- Youth Offending team – 46

10. Processing for a Law Enforcement purpose (LEP)

10.1 Law Enforcement purposes are defined at S31 of the DPA 2018 as the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. The requirements for law enforcement processing are found within part 3 of the DPA 2018.

10.2 The DPA 2018 defines the requirements of law enforcement processing by applying the format of the data protection principles at article 5 of UKGDPR to it. They are located at Part 3, Chapter 2, Ss34 – 40 of the Act. The principles are summarised below with links to the full content. The controller in relation to personal data is responsible for, and must be able to demonstrate, compliance with this Chapter (S34(3) DPA 2018).

10.2.1 The ICO provides guidance about Law Enforcement principles

10.3 Overview [of principles] and general duty of controller. S34 DPA 2018

10.3.1 1st principle - processing to be lawful and fair. S35 DPA 2018

DPA 2018, S35	Commentary
S35(2), Processing of personal data for any of the law enforcement purposes is lawful only if and to the extent that it is based on law and either the data subject has given consent to the processing for that purpose or the processing is necessary for the performance of a task carried out for that purpose by a competent authority.	A statute or common law must exist to qualify the processing for it to be lawful. That must be identified or suspected to apply before processing takes place. Obtaining witness evidence and obtaining accounts from suspects is with their consent because neither can usually be forced. Further processing of that personal data such as forwarding it to other roles within Merseyside Police or the CPS or others is with implied consent or is necessary for the performance of a task for the law enforcement purpose. Merseyside Police is a competent authority.
S35(3) In addition, where the processing for any of the law enforcement purposes is **sensitive processing**, the processing is permitted only in the two cases set out in subsections (4) and (5).	S35(8) In this section (S35), "sensitive processing" means— (a)the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership

	(b)the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual (c)the processing of data concerning health (d)the processing of data concerning an individual's sex life or sexual orientation.
S35(4) The first case is where— (a)the data subject has given consent to the processing for the law enforcement purpose as mentioned in subsection (2)(a), and (b)at the time when the processing is carried out, the controller has an appropriate policy document in place (see section 42).	This applies to processing personal data with consent. Merseyside Police has an Appropriate Policy Document (APD). It is the responsibility of the Data Protection Officer to keep the APD current and up to date.
(5) The second case is where— (a)the processing is strictly necessary for the law enforcement purpose, (b)the processing meets at least one of the conditions in Schedule 8, and (c)at the time when the processing is carried out, the controller has an appropriate policy document in place (see section 42).	Personal data may be processed without consent if strictly necessary for an LEP, but we must identify and record a condition from DPA 2018 schedule 8 for it to be lawful. That may be achieved for mainstream processing by completion of a Record of Processing Activity (ROPA) document available on the iForce page Information Assurance and Data Protection (sharepoint.com) Completed ROPAs will be available on the same page link above for access to ensure that an existing ROPA accounts for the process being followed. In the absence of an existing applicable ROPA, a new one must be completed and registered with the Information Assurance Unit. The Information Compliance Officers are available to assist in this regard. The email address for contact is Information.security@merseyside.police.uk Further detail about schedule 8 is below. Merseyside Police has an Appropriate Policy Document (APD). It is the responsibility of the Data Protection Officer to keep the APD current and up to date.
Schedule 8 DPA 2018	The conditions in schedule 8 are: Statutory etc purposes Administration of justice Protecting individual's vital interest Safeguarding of children and of individuals at risk Personal data already in the public domain Legal claims

	Judicial acts Preventing fraud Archiving etc The conditions must be read in full using the link to ensure that it is applicable in the circumstances.

10.3.2 2nd principle - processing to be specified, explicit and legitimate S36 DPA 2018

S36 DPA 2018	Commentary
(1) The second data protection principle is that— (a)the law enforcement purpose for which personal data is collected on any occasion must be **specified, explicit and legitimate**, and (b)personal data so collected must not be processed in a manner that is incompatible with the purpose for which it was collected.	(a) The terms specified, explicit and legitimate are perhaps best explained by the terms used in the 3rd principle as being adequate, relevant, and not excessive. Do not collect personal data that is superfluous to the investigation. (b) compatibility may have to be considered in a case-by-case basis. An example is that we collect personal data for an investigation, but the CPS use the same personal data for a prosecution. That is not considered incompatible. The rest of this section provides more clarity.
(2) Paragraph (b) of the second data protection principle is subject to subsections (3) and (4).	This will provide instances where personal data collected for an LEP is permissible.
(3) Personal data collected for a law enforcement purpose may be processed for any other law enforcement purpose (whether by the controller that collected the data or by another controller) provided that— (a)the controller is authorised by law to process the data for the other purpose, and (b)the processing is necessary and proportionate to that other purpose.	(3) this allows us to use personal data collected from previous occurrences in other occurrences for LEP as long as the 'new' purpose is also lawful, and the processing is proportionate to that investigation. It also allows us to share the personal data with other controller that lead other competent authorities. This is where the advice in parts 9.10 to 9.12 about identifying competent authorities when sharing LEP personal data becomes relevant.
(4) Personal data collected for any of the law enforcement purposes may not be processed for a purpose that is not a law enforcement purpose unless the processing is authorised by law.	We are regularly asked for personal data that has been gathered as part of a law enforcement purpose by regulatory bodies or local authorities. In order to do so lawfully, those requesting personal data from us must identify the legislation they are complying with to justify their request. Only when we know and accept that legislation as justifying disclosure should we respond with the requested data.

10.3.3 S37, 3rd principle - personal data to be adequate, relevant, and not excessive

S37 DPA 2018	Commentary
personal data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed.	It is important to get this right at the point of gathering personal data for a LEP (or general purposes) because the electronic systems into which the personal data is recorded has limited or no functionality to edit out irrelevant or excessive personal data. Editing is restricted or impossible as a matter of preserving the integrity of the information collected.

10.3.4 S38(1), 4th principle - personal data to be accurate and kept up to date.

S.38 DPA 2018	Commentary
(1) The fourth data protection principle is that— (a)personal data processed for any of the law enforcement purposes must be accurate and, where necessary, kept up to date, and (b)every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay.	Accuracy refers to accurate recording of personal data. Personal data gathered during an investigation comes in various shades of truth from honest misapprehension or misperception through to premeditated lies. As long as we take an accurate record of what we are told or obtain in statements or other documents, they are accurate for these purposes. Indeed, it may be the accuracy or inaccuracy of accounts provided which assist in assessing the credibility of a witness or suspect. A statement after signature must not be erased as a matter of integrity for the investigation or case. Any rectification must be achieved by obtaining a supplementary statement to correct an earlier mistake or inaccuracy. Inaccuracy may also be caused by mis-scanning paper documents into an electronic format when a page or part of a page fails to scan. The electronic version will then be an inaccurate version of the original. A reasonable step would be to ensure that this example has not happened by proofreading the scanned version against the original.
(2) In processing personal data for any of the law enforcement purposes, personal data based on facts must, so far as possible, be distinguished from personal data based on personal assessments.	We do not have a system of grading the quality or veracity of statements in the same way that we grade intelligence. That is a matter for investigators, CPS, Courts, and juries to decide upon. However, when gathering evidence, it will assist compliance with this requirement to prompt witnesses to evidence their statements with additional information that will indicate why what they are saying is fact rather than a perception or personal assessment.

	Also, previous, or subsequent enquiries may assist in determining how factual a witness or suspects accounts may be.
(3) In processing personal data for any of the law enforcement purposes, a clear distinction must, where relevant and as far as possible, be made between personal data relating to different categories of data subject, such as— (a)persons suspected of having committed or being about to commit a criminal offence (b)persons convicted of a criminal offence (c)persons who are or may be victims of a criminal offence (d)witnesses or other persons with information about offences.	The Niche system is used for law enforcement investigations It categorises persons involved in the case as, for example witness, aggrieved, suspect, in respect of the individual occurrence. Corvus also categorises the status of an individual in a case by recording 'roles' within an occurrence and further categorising types of events or occurrences as for example 'Crime offender record or crime complainant record. Where LEP investigations are administered on any other system it must have, as far as possible a similar capability.
(4) All reasonable steps must be taken to ensure that personal data which are inaccurate, incomplete or no longer up to date is not transmitted or made available for any of the law enforcement purposes.	This is achieved by providing supplementary information with transmitted to ensure it is accurate, complete, and up to date. Such updates should be recorded in the occurrence or case (OEL) so that we have a complete record of everything provided. See also Logging requirements.
(5) For that purpose— (a)the quality of personal data must be verified before it is transmitted or made available, (b)in all transmissions of personal data, the necessary information enabling the recipient to assess the degree of accuracy, completeness and reliability of the data and the extent to which it is up to date must be included, and (c)if, after personal data has been transmitted, it emerges that the data was incorrect or that the transmission was unlawful, the recipient must be notified without delay.	(a) and (b) are self-explanatory. (c) to meet such requirements there must be a record of what personal data has previously been transmitted and to who etc. This is achievable by having the detail of previous sharing available in the Logging requirements arrangements.

10.3.5 S39(1), 5th principle - personal data to be kept for no longer than is necessary

S39 DPA 2018	Commentary
(1) The fifth data protection principle is that personal data processed for	This requirement is the responsibility of the Force Records Manager to comply with the

any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed.	requirements of the Management of Police Information (MOPI) guidance and NPCC/Force Review, Retention and Disposal (RRD) schedules. The data subjects right to erasure will be referred to the Data Protection Officer for attention. General users will not attempt to dispose of any records nor retain records that should be destroyed of their own volition. In certain circumstances doing so may amount to a criminal offence (s173 DPA 2018).
(2) Appropriate time limits must be established for the periodic review of the need for the continued storage of personal data for any of the law enforcement purposes.	These time limits are established in MOPI and RRD schedules. The Force Records Manager will comply with this requirement.

10.3.6 S40, 6th principle personal data to be processed in a secure manner.

S40 DPA 2018	
Personal data processed for any of the law enforcement purposes must be so processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, "appropriate security" includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage).	For electronic systems, appropriate security of personal data is the responsibility of the ICT Department to ensure. Persons transmitting personal data as part of their role must ensure that appropriate security measures are deployed in email and hard copy transfers. The documents must be appropriately marked. See the Government Security Classification Scheme, GSCS policy and procedure for guidance. on iForce page The email system used by Merseyside Police is appropriately secure for classifications of information up to OFFICIAL-Sensitive. Departments routinely dealing with information of a higher sensitivity will have their own arrangements. Consult the Information Assurance Coordinator for advice in the event of any concerns information.security@merseyside.police.uk

10.3.7 Safeguards: archiving

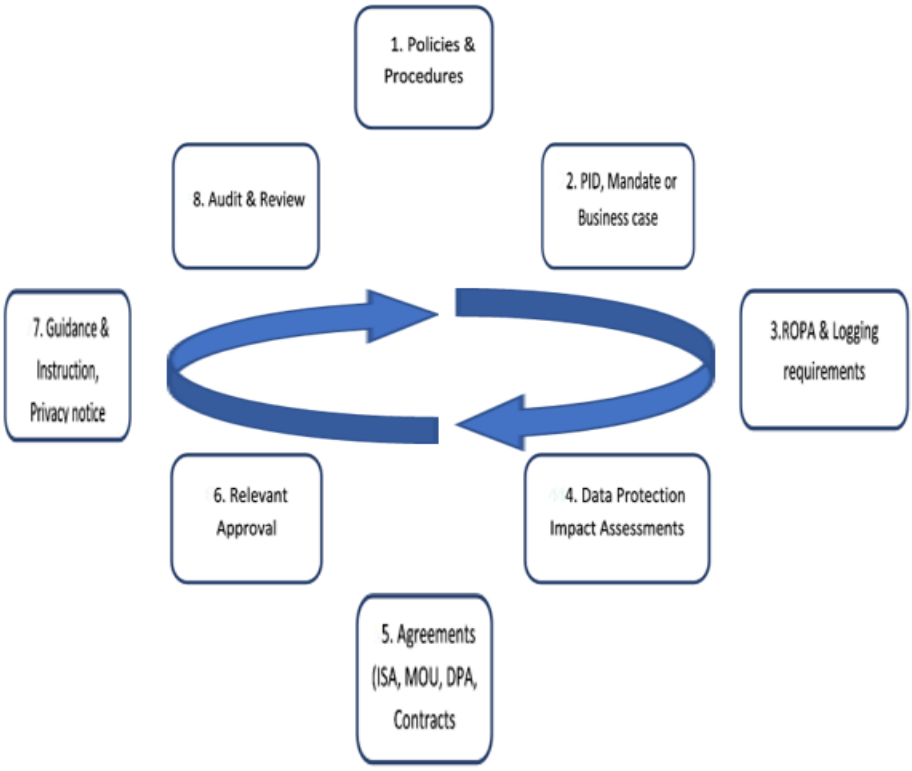
S41 of the DPA 2018 requires that processing of personal data for a law enforcement purpose where the processing is necessary for archiving purposes in the public interest, or scientific or historical research purposes, or for statistical purposes then the processing is not permitted if it is carried out for the purposes of, or in connection with, measures or decisions with respect to a particular data subject, or it is likely to cause substantial damage or substantial distress to a data subject.

10.3.8 Safeguards: sensitive processing

S42 of DPA 2018 requires a controller to have an appropriate policy document in place when carrying out sensitive processing of personal data for law enforcement purposes. The creation and maintenance of this document and full compliance with S2 is the responsibility of the Data Protection Officer. In addition, a safeguards policy including details of the requirements of the appropriate policy documents should be made available to the pubic via the Force website.

11. Information Governance and Compliance Cycle

11.1 To achieve compliance with the UKGDPR and DPA 2018 there are a number of documents and processes which are statutory requirements. They should be completed in a logical order because some rely upon the existence of others to maximise their effectiveness and value. When completed, they serve to ensure compliance with the legal requirements, improve governance of processing of personal data and increases compliance with the legislation. Because all of the documents will require periodic review, either triggered by events or at a set time for review, it may be viewed as a cycle as depicted below. It is called the Information Governance & Compliance Cycle. There are links in part 5 of this procedure that provide APP and ICO guidance about some of these documents or phases of the cycle.



11.2 Policies & Procedures (1)

11.2.1 Policy and procedure is depicted as the first step in the cycle because that will the statement of intent and guidance on how it is to be implemented. It may be a new policy when something is introduced, or a changed policy resulting from a review or audit or triggered by an event which requires a change to the policy or procedure. All policies and procedure are required to be reviewed every three years unless triggered during that period.

11.3 Project Initiation Documents, Mandates, Business Cases (2)

11.3.1 A project initiation document (PID) is usually the first documentation borne out an idea or initiative. This may be described as an outline business case. Different departments use different terms. If accepted, then it will become a project mandate or full business case. This is the blueprint for a change or initiative to progress.

11.4 ROPA & Logging requirements (3)

11.4.1 A Record of Processing Activity is a legal requirement under S61 of the DPA 2018. It is to test the lawfulness of intended processing and if that test is passed to account for the lawfulness of processing of personal data in a specified process. It will reflect what will be done with personal data, how and why. A template to complete this obligation is available on this iForce page Information Assurance and Data Protection (sharepoint.com)
Every general or law enforcement process must have a ROPA which must be periodically reviewed or triggered for review by any change in the processing for that purpose.

11.4.2 The logging requirement is a legal requirement under S62 of the DPA 2018. It is required whenever personal data is shared for a law enforcement purpose. It is data subject specific for each time personal data is processed as opposed to merely reflecting a repeated process. This is an arduous task. There is an excel workbook to account for the logging requirements available on this iForce page to achieve compliance. Information Assurance and Data Protection (sharepoint.com)
The Force is actively engaged in exploring an automated method to fulfil this requirement.

11.5 Data Protection Impact Assessments (4)

11.5.1 DPIAs is a legal requirement of S64 of the DPA 2018. It is intended to assess the impact that an intended or process in use has on data subjects. In order to do this successfully, it is necessary to understand what is to be done with the personal data. Therefore, reference to a completed ROPA will assist your assessment. This is why the ROPA must be completed before a DPIA is attempted. Any risks which are exposed by a DPIA must be accepted or rejected by a relevant role, as specified in the template. To assist in this, the requirements of the ROPA have been incorporated into the DPIA template for use when no ROPA already exists. It is available on this iForce page. Information Assurance and Data Protection (sharepoint.com)

11.6 Agreements (5)

11.6.1 Whenever Merseyside Police shares personal data with an external body as a one off or on an ad-hoc basis then the purpose and justification for doing so must be recorded with relevant documentation. In the case of law enforcement purposes, it is part of the logging requirements mentioned at 11.4 above.

11.6.2 Whenever Merseyside Police shares personal data with an external body on a regular basis, a written formal agreement must be created and signed by all relevant parties to it. They may be referred to as Information Sharing Agreements, Memorandum of Understanding, Data Processing Agreements or Data Processing Contracts dependent upon the relationship between the parties.

11.6.3 The ICO as a requirement of S121 of the DPA 2018 has published a Data sharing code of practice which will provide guidance. Additionally, there is an Information Sharing Agreement template on this iForce page. Information Assurance and Data Protection (sharepoint.com)
Other formats of agreements are available upon request to information.security@merseyside.police.uk

11.7 Relevant Approval (6)

11.7.1 All of the documents mention in this part are subject of relevant approval which must be explicit within the form. Information Asset Owners must be made aware of how the information asset that they 'own' is being processed and approve or reject the proposed processing. Some of the documents also require perusal and input by the Data Protection Officer. On occasions, the SIRO will also be consulted and in relevant circumstances, the ICO must also be consulted (S65 DPA 2018) prior to implementation of a process. The latter will be achieved by liaison with the Data Protection Officer as Force SPOC with the ICO.

11.8 Guidance, Instruction and Privacy Notices (7)

11.8.1 When a process has been established and approved consideration must be given to providing those required to implement the process with applicable and ample training to carry out the process with confidence. It must be readily available to them by an appropriate method.

11.8.2 The Data Protection Officer will review existing privacy notices to ensure that the process is appropriately included in the privacy notice, making amendments as required. The Appropriate Policy Documents will be reviewed in a similar way for law enforcement processes. The Data Protection Officer will also regularly review the privacy information provided to data subjects to ensure it remains accurate, relevant, and current. A historical log of privacy notices should be kept, including the dates on when any changes were made, to allow it to be known what privacy information was provided to individuals at the time of data collection.

11.8.3 When conducting the data mapping exercise of existing processing activities as well as any new processing activity, the Information Assurance Team should ensure that the process includes reviewing existing privacy information to ensure it accurately reflects the processing carried out

11.9 Audit & Review

11.9.1 Shared Internal Audit will carry out periodic review around data protection compliance. Additionally, Information Compliance Officers will conduct regular structured assurance mapping using the assurance mapping template. Information Asset Owners will conduct regular reviews of compliance with compliance as part of the governance of the information that they 'own'.

12. Requests for personal data to external agencies or bodies

12.1 Requests for personal data may be made to external agencies using the form Request to external organisation for information which is available on this iForce page Information Assurance and Data Protection (sharepoint.com)

13. Notification

13.1 The National regulator for the supervision of Data Protection is the Information Commissioner to whom the Chief Constable notifies his purposes for processing personal data annually and pays a fee.

13.2 The Protection Officer is responsible for such notification and renewal of the registration.

14. Data Subject Rights

14.1 The rights of data subjects are available at articles 13 to 23 of the UKGDPR and Ss 43 to 54 of the DPA 2018.

14.2 Subject Access requests for the specifies personal data about the data subject made by the data subject or their representative. They will be administered, and responses provided by the data analyst in the Data Access Unit in Criminal Justice.

14.3 All remaining data subject rights will be overseen and responded to by the Data Protection Officer or their delegates. This includes creation and oversight of appropriate processes that all relevant staff will need to engage with.

14.4 Any person who receives any such requests must not respond directly with the data subject. Instead, subject access requests must be forwarded to dataprotection@merseyside.police.uk Other data subject requests must be forwarded to data.protection.officer@merseyside.police.uk In either case it must be done without any delay because, in usual circumstances, as response to the data subject is required within one calendar month.

14.5 Although staff response is summarised in 14.4 above, the Data Protection Officer will ensure that there is a documented procedure for individuals to challenge the accuracy of their personal data and for all staff on how to handle requests for rectification. The documented rectification procedure should set out the requirements of s.46 DPA18 including the need for a supplementary statement. In addition, the procedure should include the statutory timescale for responding to such a request. The procedure should be communicated and readily available for all staff to access via iForce on this page Information Assurance and Data Protection (sharepoint.com)

14.6 The Data Protection Officer must have a clear method for identifying when personal information has been shared with a third party, documented in working practices for handling rectification requests.
Furthermore, there will be a defined process to notify competent authorities from where personal data originated in the event of a rectification request being processed.

14.7 Staff who may share personal data with third parties must record this information on any systems in which personal data is stored in addition to recording the transaction within the logging requirements arrangements when sharing personal data for a law enforcement purpose.

14.8 The Data Protection Officer will maintain a documented procedure for individuals and staff to follow when handling a request for erasure. Quite simply, any data subject rights request including requests for erasure must be referred to the Data Protection Officer who will have a documented procedure to respond to such requests including the requirement to erase or restrict the processing of personal data where it would infringe s.47(1) DPA18. If deletion is not technically possible, the personal data will be put 'beyond use' the process for doing so documented. The DPO will also document their process for informing third parties in a timely manner with whom the data has been shared in compliance with Article 17 UK GDPR and s.47 DPA18.

14.9 The Data Protection Officer in liaison with the Information Assurance Coordinator must have processes and guidance to follow when notifying individuals of a PDB. For law enforcement processing, where the provision of information about the breach is restricted wholly or partly, the procedure should ensure that the restriction is applied appropriately and consistently with the decision to restrict the provision of information documented. A template breach notification letter to include the contact details for the DPO, the likely consequences for the individual and any action they can take to safeguard themselves will be used in compliance with Article 32 UK GDPR and s.68 DPA18.

15. Advice and Guidance

15.1 The Data Protection Officer, Information Assurance Coordinator and the Information Compliance Officers will provide relevant advice as part of their roles. They are:

DPO – Ian Boyham – X78317 – Ian.Boyham@merseyside.police.uk
IAC – Phil Caddick – X71399 – Phillip.Caddick@merseyside.police.uk
Information Compliance Officer – Janet Fogg – X78543 – Janet.Fogg@merseyside.police.uk
Information Compliance Officer – Michelle McMurrie – x78438 – Michelle.McMurrie@merseyside.police.uk

15.2 The above roles will provide relevant guidance in other media and make them available to the Force on the iForce page
Information Assurance and Data Protection (sharepoint.com)

15.3 'Live' or real personal data must never be used as part of any training material.

15.4 The national training courses 'Managing Information' and its' refresher training is a mandatory requirement as ordered by the SIRO and should be repeated annually.