

Merseyside Police

Appropriate Policy Document and additional safeguards

Version History

<i>Version Number</i>	<i>Date</i>	<i>Rational behind amending/updating policy or procedure.</i>	<i>Policy Owner details</i>
V.1	21/05/2018	First created to comply with requirement of S.42 of the DPA 2018	Data Protection Officer, Merseyside Police
V.	21/11/2022	Amended to comply with ICO audit recommendations.	Data Protection Officer, Merseyside Police

1-Introduction

In order to process personal data lawfully, it must be done in compliance with the data protection principles as defined in Article 5 of the UK General Data Protection Regulations, hereafter referred to as 'UK GDPR' and meet a condition in Article 6, as supplemented by S.8 of the Data Protection Act 2018, hereafter referred to as the 'DPA', in respect of processing in the public interest. To lawfully process special categories of personal data, we must comply with a condition in Article 9 of the UK GDPR and sections 10 and 11 of the DPA 2018. Section 10 requires identification of a purpose as contained in parts 1, 2 or 3 of Schedule 1 of the DPA.

When processing for law enforcement purpose, that is achieved lawfully by compliance with S.35(4) & (5), section 42 and Schedule 1, part 4 (38) of the DPA. That requires the consent of the data subject or at least one of the conditions of schedule 8 of the DPA, AND at the time of such processing, we are required to have an 'appropriate policy document. This document is our appropriate policy document as required by S.42 of the DPA. It explains what special category (sensitive) personal data and criminal offence personal data are, our retention and erasure policies in relation to the sensitive processing and how we review that personal data and this document.

2-What personal data is.

"Personal data" means any information relating to an identified or identifiable living individual (subject to subsection (14)(c)).

"Identifiable living individual" means a living individual who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data or an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual. (DPA S.3(2) & (3).

3-What Special Category personal data is.

Special Category personal data that may include detail about:

- Physical or mental health details
- Racial or ethnic origin
- Trade union membership
- Political opinions
- Religious or other beliefs
- Sexual and sexual orientation
- DNA fingerprints and other genetic or biometric samples.

(Article 9 UK GDPR)

4-What criminal conviction and offence personal data is

Personal data relating to criminal convictions and offences including:

- Offences and alleged offences
- Criminal proceedings, outcomes and sentences
- Criminal intelligence

(Article 10 UK GDPR and Ss. 10 & 11 of DPA)

5-What the law enforcement purposes are

“Law enforcement purposes” are defined as 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. (S.31 of DPA)

As a Police force, it is necessary to carry out sensitive processing to fulfil the functions of a law enforcement agency as both a competent authority (as identified in Schedule 7 of DPA) and being responsible for the policing of the Merseyside Police area.

6-DPA, S.35, the first data protection principle (lawful and fair). The conditions for processing sensitive data for law enforcement purposes.

Section 35(4) and (5) of the Act states that sensitive processing for law enforcement purposes is permitted in only two cases:

*a) the data subject has given consent to the processing for the specific purpose **and** at the time the processing is carried out, the controller has an appropriate policy document (APD) in place*

or

*b) the processing is strictly necessary for a law enforcement purpose, the processing meets at least one condition in Schedule 8 of the Act **and** at the time the processing is carried out, the controller has an APD in place. If either of these two conditions are met, and we have an APD (this document) the sensitive processing will be lawful.*

In addition to schedule 8 mentioned below, Schedule 1 of the DPA establishes conditions that permit the processing of the special categories of personal data and criminal convictions etc [and offences] data outside of the law enforcement purposes.

Part 4 of Schedule 1 makes provision for the establishment, content and maintenance of “appropriate policy documentation” where such documentation is required by a condition in Parts 1, 2 or 3 of schedule 1. An appropriate policy document is also required or inferred at GDPR Article 5(2) and DPA section 34(3) for a demonstration of compliance and DPA Sections 35 principle 1 and 42(1) (Safeguards: sensitive processing).

When processing of special categories of personal data take place for a law enforcement purpose without the consent of the data subject, a condition under schedule 8 must be identified for the processing to be lawful.

7-Principles relating to processing of personal data for law enforcement purposes

Principles relating to processing of personal data. Personal data shall be:	Explanation of Compliance
(Principle (a): lawful and fair, S.35(1) DPA the processing of personal data for any of the law enforcement purposes must be lawful and fair.	Processing special categories of personal data and criminal conviction and offence data must be lawful, fair and transparent (as does processing of any personal data). It is only lawful if and to the extent it is based on law and either the data subject has given their consent for the processing, or the processing meets at least one of the conditions in Schedule 1. (DPA s.10(2)(3)(5)) Our processing for purposes of substantial public interest is necessary for the exercise of a function conferred on a law enforcement agency by legislation To ensure that the processing complies with this principle we conduct Data Processing Impact Assessments (S.64 DPA) and maintain Records of Processing Activities (S.61 DPA) and publish privacy notices on our external website.
Principle (b): purpose limitation, S.36(1) DPA (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.	Sensitive processing will be restricted to only that which is necessary for the relevant law enforcement purpose, and it will not be used for a matter which is not a law enforcement purpose unless that use is authorised by law. It may, however, be used for another law enforcement purpose by us or another organisation that is authorised to carry out law enforcement or regulatory processing. If we are sharing data with another controller, we will ensure and document that they are authorised by law to process the data for their purpose. If this is done regularly, we will have a sharing agreement which documents this. We will not process personal data for purposes incompatible with the original purpose it was collected for.

Principle (c): data minimisation S.37 DPA 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.	We collect personal data necessary for the relevant purposes and ensure it is not excessive. The information we process is necessary for and proportionate to our purposes. Where personal data is provided to us or obtained by us, but is not relevant to our stated purposes, we will erase it. The detail to comply with this principle is in our Records of Processing document (tab 11) to prompt avoidance of excessive data processing. It is subject to assessment by completion of a DPIA at the commencement of processing information for a specified purpose and later upon review.
Principle (d): accuracy S.38 DPA (paraphrased) (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) personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay. (2) personal data based on facts must, so far as possible, be distinguished from personal data based on personal assessments. (3) 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. (4) personal data which is inaccurate, incomplete or no longer up to date is not transmitted or made available for any of the law enforcement purposes.	We will ensure as far as possible that the data we hold is accurate and kept up to date. In some circumstances we may need to keep factually inaccurate information e.g., in a statement from a victim, witness or alleged perpetrator, because the data is accurate to the extent that it is what we have been provided with, even though it may not necessarily be true. All officers and staff are made aware of the need for accuracy and are responsible for the accuracy of the personal data they process. Checks are carried out on the accuracy of data during audits and line manager checks. Personal data found to be inaccurate will be rectified or erased whenever possible. Where this is not possible, there will be an addendum to that personal data advising of the inaccuracy. When necessary, the processing will be restricted in accordance with Sections 46 to 48 of the DPA. This will ensure that data will not be transmitted or made available for any of the law enforcement purposes. If inaccurate personal data has been previously disclosed to other parties, the recipient(s) will be advised of this as soon as practicable after discovering the inaccuracy. Where we become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed, we will take every reasonable step to ensure that data is erased or rectified without delay. If we decide not to either erase or rectify it, for example because the lawful basis we rely on to process the data means these rights don't apply, we will document our decision. We will respond to inaccuracies brought to our attention by data subjects when exercising their rights.

(5) 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.	
Principle (e): storage limitation S.39 DPA (1) personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed. (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.	Merseyside Police retains all personal data in accordance with the NPCC and its' own retention schedules which is aligned to the Management of Police Information (MOPI) guidance retention periods as described in Appendix 4 of MOPI and adheres to the National retention assessment criteria (NRAC) for offender data. It may also retain personal data under statute, rule of law or order of a Court or Tribunal. It will be made available upon request to the Information Commissioner (as the Supervisory Authority) for up to 6 months after the data controller ceases processing those data. Merseyside Police maintains and reviews a Records Management Policy and Procedure which is of relevance to this principle.
Principle (f): integrity and confidentiality (security) S.40 DPA 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).	We have developed and implemented appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. Technical measures – We apply the information security standards set for the National Policing Community by the Cabinet Office and the Home Office and work with the Police Digital Service and the National Monitoring Centre to maintain and continuously improve our security arrangements. This includes encryption, firewalls, anti-virus software, IT health checks, vulnerability assessment and penetration process, user authentication, role based and password controlled access, technical assurance and technical audits and end point management. We adhere to security standards which surpass the requirements of ISO 27001 and the Government Security Framework. It has relevant codes of connection accreditations for a number of different processing activities.

	Organisational measures - Personal data and other information is protected using the Government Security Classification Scheme (GSCS). There is a robust security breach reporting process in being in accordance with our Security and Personal Data Breach Notification Policy and Procedure. Information Management training is delivered to every member of staff as a mandatory requirement in respect of the DPA 2018 and the UK GDPR to increase awareness and avoid data breaches. The training is refreshed annually. All new staff, officers and contractors are vetted prior to being given access to the information, systems and records. The vetting is subject to periodic review. Officers and staff receive training in how to use police systems before being granted access. Buildings are kept physically secure with access only being granted to individuals who require it in accordance with our Physical Security Procedures document
--	---

8-Conditions for processing special category and criminal conviction and offence etc., personal data.

In order to process personal data lawfully, it must be done in compliance with the data protection principles as defined in Article 5 of the UK GDPR and meet a condition in Article 6, as supplemented by S.8 of the DPA 2018 in respect of processing in the public interest.

To lawfully process special categories of personal data, we must comply with a condition in Article 9 of the UK GDPR and sections 10 and 11 of the DPA 2018. Section 10 requires identification of a purpose as contained in parts 1, 2 or 3 of Schedule 1 of the DPA.

The conditions to lawfully process special categories and criminal conviction and offence etc., personal are found at Articles 9.2 and 10 of the UKGDPR. The conditions which we would rely upon in different circumstances are reproduced below.

Article 9 – Processing of special categories of personal data.

9.1. 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.

9.2. Paragraph 1 shall not apply if one of the following applies:

9.2(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where domestic law provides that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

9.2(b) processing is 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 in so far as it is authorised by domestic law or a collective agreement pursuant to domestic law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

9.2(c) processing is 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;

9.2(e) processing relates to personal data which are manifestly made public by the data subject;

9.2(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

9.2(g) processing is necessary for reasons of substantial public interest, on the basis of 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 domestic law;

9.2(h) 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 or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

9.2(i) 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 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;

9.2(j) 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.

9.3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when 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.

9.[3A. In paragraph 3, ‘national competent bodies’ means competent bodies of the United Kingdom or a part of the United Kingdom.]

9.5. In the 2018 Act- (DPA 2018)

(a) section 10 makes provision about when the requirement in paragraph 2(b), (g), (h), (if) or (j) of this Article for authorisation by, or a basis in, domestic law is met;

(b) section 11(1) makes provision about when the processing of personal data is carried out in circumstances described in paragraph 3 of this Article.

Article 10 – Processing personal data relating to criminal convictions and offences

10.1 Processing of personal data relating to criminal convictions and offences, or related security measures based on Article 6(1) shall be carried out only under the control of official authority or

when the processing is authorised by domestic law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

10.2 In the 2018 Act-

(a) section 10 makes provision about when the requirement in paragraph 1 of this Article for authorisation by domestic law is met;

(b) section 11(2) makes provision about the meaning of “personal data relating to criminal convictions and offences or related security measures”.]

DPA 2018, S.10 Special categories of personal data and criminal convictions etc data

S.10(1) Subsections (2) and (3) make provision about the processing of personal data described in Article 9(1) of the UK GDPR (prohibition on processing of special categories of personal data) in reliance on an exception in one of the following points of Article 9(2)—

- (a) point (b) (employment, social security and social protection);
- (b) point (g) (substantial public interest);
- (c) point (h) (health and social care);
- (d) point (in) (public health);
- (e) point (j) (archiving, research and statistics).

(2) The processing meets the requirement in point (b), (h), (i) or (j) of Article 9(2) of the UK GDPR for authorisation by, or a basis in, the law of the United Kingdom or a part of the United Kingdom only if it meets a condition in Part 1 of Schedule 1.

(3) The processing meets the requirement in point (g) of Article 9(2) of the UK GDPR for a basis in the law of the United Kingdom or a part of the United Kingdom only if it meets a condition in Part 2 of Schedule 1.

(4) Subsection (5) makes provision about the processing of personal data relating to criminal convictions and offences or related security measures that is not carried out under the control of official authority.

(5) The processing meets the requirement in Article 10(1) of the UK GDPR for authorisation by the law of the United Kingdom or a part of the United Kingdom only if it meets a condition in Part 1, 2 or 3 of Schedule 1.

DPA 2018, S.11.2 Special categories of personal data etc: supplementary

11(1) deals with a circumstance which is not for law enforcement processes so is not reproduced here.

11(2) In Article 10 of the GDPR UK GDPR and section 10, references to personal data relating to criminal convictions and offences or related security measures include personal data relating to—

- (a) the alleged commission of offences by the data subject, or*
- (b) proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing.*

When processing for law enforcement purpose, that is achieved lawfully by compliance with S.35 of the DPA. That requires the consent of the data subject or at least one of the conditions of schedule 8 of the DPA, AND at the time of such processing, we are required to have an 'appropriate policy document. This document is our appropriate policy document.

The DPA Schedules

In this document, reference has been made to conditions in schedules having to be met before special category or criminal conviction or offence personal data may be processed. Below is a list of brief descriptions of the conditions. The ones more commonly used are in **bold type**

The details of the relevant conditions relied on in a variety of circumstances are listed below;

DPA Schedule 8. – This is the schedule which applies to law enforcement processing

The conditions which apply to law enforcement processing are:

1 – Statutory purposes.

Other commonly used conditions are:

3 – Protecting individual's vital interests; and

4 – Safeguarding of children and of individuals at risk.

6 – Legal Claims

8 – Preventing fraud

9 – Archiving

Merseyside Police may rely upon the following conditions for processing personal data for different processing purposes.

DPA 2018, Sch1, Pt1, 1. (1)(a)(b) & (2) - (Employment, social security and social protection)

Processing necessary for the purposes of performing or exercising obligations or rights of the controller or the data subject under employment law, social security law or the law relating to social protection. In order to meet this condition, the controller must have an appropriate policy document in place, as required under Part 4 of Schedule 1

DPA 2018 Sch1,

Pt2, 5(1) – (Substantial Public Interest Conditions)

There is a requirement for have an appropriate policy document when relying on conditions in this Part.

DPA 2018 Sch1,

Pt2, 6 (Statutory etc and government purposes)

(1) This condition is met if the processing—

(a) is necessary for a purpose listed in sub-paragraph (2), and

(b) is necessary for reasons of substantial public interest.

(2) Those purposes are—

(a) **the exercise of a function conferred on a person by an enactment or rule of law;**

(b) the exercise of a function of the Crown, a Minister of the Crown or a government department.

DPA 2018 Sch1, Part 2

7 (Administration of justice and parliamentary purposes)

8 (Equality of opportunity or treatment)

10 (Preventing or detecting unlawful acts)

11 (Protecting the public against dishonesty etc)

12 (Regulatory requirements relating to unlawful acts and dishonesty etc)

- 13 (Journalism etc in connection with unlawful acts and dishonesty etc)
- 14 (Preventing fraud)
- 15 (Suspicion of terrorist financing or money laundering)
- 17 (Counselling etc)
- 18 (Safeguarding of children and of individuals at risk)**
- 19 (Safeguarding of economic well-being of certain individuals)
- 20 (Insurance)
- 21 (Occupational pensions)
- 24 (Disclosure to elected representatives)
- 25 (Informing elected representatives about prisoners)
- 26 (Publication of legal judgments)
- 27 (Anti-doping in sport)
- 28 (Standards of behaviour in sport)

Schedule 1 Part 3 - ADDITIONAL CONDITIONS RELATING TO CRIMINAL CONVICTIONS ETC

- 29 (Consent)
- 30 (Protecting individual's vital interests)
- 32 (Personal data in the public domain)
- 33 (Legal claims)
- 34 (Judicial acts)
- 36 (Extension of conditions in Part 2 of this Schedule referring to substantial public interest)

9-Records of Processing Activities

Merseyside Police processes data in categories that require an appropriate policy documentation to be in place. Merseyside Police processes personal data for many reasons and purposes. As required by Article 30 of the UK GDPR and S.61 of the DPA, Records of Processing Activity are continuously updated and reviewed to document all processing activity. These documents identify the department or unit which processes the personal data, the purposes of processing, the types and categories of personal data involved, its' intended recipients, the conditions for lawful processing, transfers outside of the UK, its' intended retention and review period, the security measures in place for the personal data, whether a Data Processing Impact Assessment exists for the process, whether the process is addressed in the general privacy notice or if there is a bespoke privacy notice, and how compliant the process is with the principle of data protection by design and default.

10-Review, Retention or Erasure of personal data

Merseyside Police retains all personal data in accordance with the NPCC and its' own retention schedules which is aligned to the Management of Police Information (MOPI) guidance retention periods as described in Appendix 4 of MOPI and adheres to the National retention assessment criteria (NRAC) for offender data. All are designed and intended to comply with the 5th data protection principle.

It may also retain personal data under statute, rule of law or order of a Court or Tribunal. It will be made available upon request to the Information Commissioner (as the Supervisory Authority).

We will respond to requests for rectification or erasure of personal data when data subjects exercise their rights under Ss 46-48 of the DPA (along with all other data subject rights) which provides opportunities for us to review the personal data that is brought to our attention in this way. They

amount to 'triggered' rather than scheduled reviews. The rights of individuals are addressed at part 9 of our privacy notice. Although there is a data subjects rights request form in existence, we will accept data subject rights in any format.

Merseyside Police maintains and reviews a Records Management Policy and Procedure which is of relevance to this principle.

11-Accountability principle

Merseyside Police has in place appropriate technical and organisational measures to meet the requirements of accountability. These include:

- The appointment of a data protection officer who reports directly to our highest management level.
- Taking a 'data protection by design and default' approach to our activities. This is assessed very time an individual record of processing activity is created
- Maintaining documentation of our processing activities
- Adopting and implementing data protection policies and ensuring we have written contracts in place with our data processors
- Implementing appropriate security measures in relation to the personal data we process
- Carrying out data protection impact assessments for our high risk processing

We regularly review our accountability measures and update or amend them when required.

12-Retention and review of this policy

This appropriate policy document will be retained in accordance with Section 42 of the DPA. It will be made available to the ICO on request.

The policy will be reviewed on a biannual basis (or more regularly if circumstance requires) and updated as necessary at these reviews. Records of Processing Activities are also reviewed on a regular basis which may prompt changes to the APD during interim periods.

There is a version history table in this document to record all version changes.

There are a number of information systems which will not currently allow for the deletion of data in isolation from other data to which it is linked (an integrated system). The main system used is Niche which has this characteristic. This is the same problem for all Forces with this system. The contractor (Minerva) is aware of this problem and is investigating a solution. The ICO is also aware of this problem with compliance. A temporary fix is present by IT changing the access control levels so that users cannot access or see the data. Merseyside Police will continue to identify and correct any other areas of non-compliance as the Information Asset Register is reviewed and brought up to date. This includes an issue of logging in accordance with S.62 DPA which is being explored. These matters are present within the Information Risk Management register and subject to regular monitoring and review with a view to compliance.