Policy

Alliance Data Protection Policy			
J-P-013 **(formerly known as SA045)**			
Version	1.1	**Host Force**	Devon & Cornwall Police
Effective date	12/07/2022	**Host Policy Unit**	Devon & Cornwall Police Policy Unit
Version date	19/07/2022	**Policy Owner**	Head of Alliance Information Management
Review date	12/07/2023	**Policy Author**	Alliance Data Protection and Information Sharing Manager (DCP)
Associated Procedures	Alliance Data Protection Procedure J-Pr-003		

1. Policy Summary

1.1 Devon and Cornwall (DCP) and Dorset Police (DP) have a statutory obligation to process personal data in accordance with the provisions of the UK General Data Protection Regulation (GDPR) in respect of non-law enforcement processing and the Data Protection Act 2018 (DPA) in respect of law enforcement processing. For ease of reference these will be collectively referred to as 'Data Protection legislation' for the remainder of this document.

1.2 For the purpose of this policy, 'data' and 'information' shall have the same meaning.

1.3 This policy applies to individuals at all levels of both Forces including Police Officers, Police Staff, Special Constabulary, Police Community Support Officers (PCSO), temporary staff and 3rd parties (for example but not necessarily limited to partner agency staff, consultants, contractors and volunteers) who have authorised access to personal data which is held by either Force.

1.4 This policy is a joint policy applicable to both DCP and DP Police forces. This policy supersedes SA045 (formerly DP - P09:2007 Data Protection Policy and Procedure and DCP – D031 Data Protection Policy).

2. Purpose, Standards and Legal Basis

2.1 Both Forces are required to abide by the DPA and where it is influenced by other legislation including the below;

2.2 The requirement to comply with this legislation shall be devolved to employees and agents of the relevant Force, who may be held personally accountable for any breaches.

- Crime and Disorder Act 1998
- Police Act 1996
- Coroners and Justice Act 2009
- The Computer Misuse Act 1990
- The Health and Safety at Work Act 1974
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- Rehabilitation of Offenders Act 1974
- Management of Police Information MOPI

2.3 Internal and external equality and diversity issues have also been considered to ensure compliance with Equality legislation and policies. Adherence to this document will therefore ensure compliance with all relevant legislation and internal policies.

3. Roles and Responsibilities

3.1 It is the responsibility of all police officers, police staff, special constables and police volunteers to monitor both their own and works colleague's adherence to this policy. Where it is believed that someone is non-compliant with the policy the Data Protection Officer (DPO) in the respective force should be informed in the first instance. The DPO will also monitor the effectiveness of this policy, reporting to the Joint Information Board where required.

4. Policy Information

4.1 This policy applies to individuals at all levels of both Forces including Police Officers, Police Staff, Special Constabulary, Police Community Support Officers (PCSO), temporary staff and 3rd parties (for example but not necessarily limited to partner agency staff, consultants, contractors and volunteers) who have authorised access to personal data which is held by either Force.

4.2 All DCP and DP Officers/Police Staff, Special Constabulary, Police Community Support Officers (PCSO), temporary staff and 3rd parties (for example but not necessarily limited to partner agency staff, consultants, contractors and volunteers) must have a clear understanding of their personal responsibilities under data protection legislation and how this affects the processing of personal data. The data protection team can be contacted for help or advice - Middlemoor 01392 303622 or

Winfrith 01202 223810 or by email
dataprotectionalliance@devonandcornwall.pnn.police.uk

4.3 Individuals described above occupy a privileged position with regard to the information they have access to. The public must have confidence in the ability of the police service to protect the confidentiality of all the information that it holds as part of its policing function. The damage done to the reputation of the service by an individual who is found to have committed a breach by unlawfully accessing, disclosing, holding or processing personal data cannot be overstated and this detracts from the credibility of the service in this crucial area.

4.4 Both forces are committed to protecting the rights of individuals with regard to the processing of personal data. DCP and DP will take criminal and/or disciplinary action against any category of person mentioned above who wilfully, without authority or defined policing purpose or other statutory or business purpose, accesses and/or misuses personal data held by either Force. Any use of personal data that does not have a defined policing or other statutory or business purpose is likely to constitute a misuse.

4.5 All personnel shall comply with relevant Force and Alliance Policy. This Policy is supported by a series of Data Protection procedures and Information Sharing Agreements (ISAs) providing more detailed guidance as required. Failure to comply with Force/Alliance Policy, or failure to follow relevant guidance, may result in criminal and/or disciplinary action.

4.6 **Data Protection key definitions**
4.6.1 Controller means the person who determines the manner and purpose for which personal data is processed; The Chief Constable for each Force is Controller.

4.6.2 Data Protection Officer (DPO) means the person designated by the controller of each Force who advises on and monitors compliance with the DPA. The DPO role, tasks, position and responsibilities are set out in the DPA.

4.6.3 Processor means any third party (other than an employee of the controller) who processes personal data on behalf of the controller.

4.6.4 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. Information about a deceased person does not constitute personal data.

4.6.5 Special Category data means racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, 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.

4.6.6 Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

4.6.7 General processing GDPR and Part 2 of the DPA relates to general processing and covers police support functions such as the People Portfolio (including Occupational Health and Health & Safety), Occupational Health, Finance and Payroll (including pensions), Estates, ICT and Procurement. GDPR does not apply to the processing of personal data by Devon and Cornwall and Dorset Police (as a competent authority) for Law Enforcement purposes.

4.6.8 Law Enforcement processing - Part 3 of the DPA relates to the processing of personal data by a competent authority for Law Enforcement purposes - 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.

4.7 **Data Protection Principles**

	General Processing	**Law Enforcement Processing**
Principle 1	Lawfulness, fairness and transparency	Lawful and fair
Principle 2	Purpose limitation	Specified explicit and legitimate
Principle 3	Data minimisation	Adequate, relevant and not excessive
Principle 4	Accuracy	Accurate, up to date
Principle 5	Storage limitation	Kept no longer than is necessary
Principle 6	Security, integrity and confidentiality	Ensure appropriate security

5. Monitoring and Review

5.1 Review and amendments will be coordinated by the Policy Unit.

5.2 The Policy Owner has overall responsibility for ensuring the content of the Policy is appropriate and up to date.

5.3 This Policy will be reviewed once a year subject to legislation/process changes.

6. Associated Documents

Policy and Procedure

- Alliance Information Management Policies and Procedures

SharePoint

- Alliance Data Protection Sharepoint page
- UK General Data Protection Regulations GDPR/ Data Protection Act 2018 DPA
- Vision, Mission & Values (DCP)
- Vision, Purpose & Priorities (DP)
- Human Rights Legislation
- Records Management (DCP)
- Records Management (DP)
- Freedom of Information Act 2000 (FOIA)
- Government Security Classification (GSC)
- UK General Data Protection Regulation /Data Protection Act (2018)
- Code of Ethics (DCP)
- Code of Ethics (DP)
- Police Staff Council Standards of Professional Behaviour

College of Policing

- National Decision Model
- Authorised Professional Practice (APP)

Other

- Information Commissioner's Office (ICO) website

7. Document History	
Present portfolio holder	Director of Legal, Reputation and Risk
Present document owner	Alliance Head of Information Management
Present owning department	Alliance Information Management
Below details required for new documents, major amendments (Dorset only) or novel/contentious amendments (Devon & Cornwall only)	
Name of board and/or Chief Officer approving	N/A
Date approved	N/A
Business Board member approving (Devon & Cornwall only when not contentious or novel)	Head of Alliance Information Management
Date approved	08/07/2022

8. Version History

Version	Date	Reason for amendments	Amended by
1.0	12/07/2022	Review of SA045 content and input into new format with new URN.	Alliance Data Protection and Information Sharing Manager (DCP)
1.1	19/07/2022	Wording changed at 4.5	Alliance Data Protection and Information Sharing Manager (DCP)

We welcome any comments or suggestions you wish to share about the content or implementation of this procedure. If you would like to make contact to discuss further, please email:
Forcepolicyandprocedures@devonandcornwall.pnn.police.uk