Heddlu • Police
DYFED-POWYS
Diogelu ein Cymuned – Safeguarding our Community

Data Protection Policy

HQ Policy Ref No: 12/01

Author: Heather Hughes
Data Protection Manager
Version: 9.0

Dept: Data Protection
Date: 1st September 2017

VERSION CONTROL

Version	Date	Author	Reason for Change
2.0	14/01/05	John Evans	Review
3.0	27/04/06	John Evans	Review
4.0	May, 2007	John Evans	Review and update Separate policy from procedure
5.0	June, 2008	John Evans	Review and update Inc. MOPI
6.0	January, 2012	Heather Hughes	Updates inc MOPI
7.0	July, 2013	Steven Mears	Review following Internal Audit
8.0	January 2014	Heather Hughes	New version
9.0	September 2017	Heather Hughes	New version

EQUALITY IMPACT ASSESSMENT

Section 4 of the Equality Act 2010 sets out the **protected characteristics** that qualify for protection under the Act as follows: Age; Disability; Gender Reassignment; Marriage and Civil Partnership; Pregnancy and Maternity; Race; Religion or Belief; Sex; Sexual Orientation.

The **public sector equality duty** places a proactive legal requirement on public bodies to have regard, in the exercise of their functions, to the need to:

- eliminate discrimination, harassment, victimisation, and any other conduct that is unlawful under the Act;
- advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it;
- foster good relations between persons who share a relevant protected characteristic and persons who do not share it.

The equality duty applies to all protected characteristics with the exception of Marriage and Civil Partnership, to which only the duty to have regard to the need to eliminate discrimination applies.

Carrying out an **equality impact assessment** involves systematically assessing the likely or actual effects of policies on people in respect of all the protected characteristics set out above.

An equality impact assessment should be carried out on any policy that is **relevant** to the public sector equality duty. An equality impact assessment template is available here.

HUMAN RIGHTS ACT CERTIFICATE OF COMPLIANCE

This policy has been drafted in accordance with the Human Rights Act and has been reviewed on the basis of its content and the supporting evidence and it is deemed compliant with that Act and the principles underpinning it.

Name:……..

Department:……

Signed:……

Freedom of Information Act 2000

Section 19 of the Freedom of Information Act 2000 places a requirement upon the Force to publish all policies on the Force website. Policies are why we do things and procedures are how we do them. A case-by-case review of procedures must be undertaken to protect law enforcement and health and safety considerations. Where a combined policy and procedure document is being produced the Force is legally required to publish the policy section and assess the procedure part to ensure no sensitive information is published.

There is a requirement therefore to review this document to establish its suitability for publication. Please identify below whether the document is suitable for publication in its entirety or not. Where it is believed that disclosure will be harmful please articulate the harm that publication would cause and highlight the relevant sections within the document. Where it is perceived that there is harm in disclosure the document should be forwarded to the FOI Unit for review.

Suitability for publication

Suitability for publication	Yes/No	Date	Signature
Document is suitable for publication in its entirety	Yes	Sept 2017	
Document is suitable for publication in part, I have identified those sections which I believe are not suitable for disclosure and have articulated below the harm which would be caused by publication.	Yes	Sept 2017	
Harm – in publication			

FOI review – to be completed by FOI Unit

Suitability for publication	Yes/No	Date	FOI Decision Maker
Document is suitable for publication in its entirety	Yes		
Document is suitable for disclosure in part and relevant redactions have been applied. A public facing version has been created.			
Once review has been undertaken FOI decision maker to return document to policy author and following sign–off document to be published within Force Publication Scheme. Any future changes to the document should be brought to the attention of the FOI Unit, as appropriate.			

Contents

Data Protection Policy

Policy Contents

This Policy has been drafted in accordance with the Human Rights Act 1998

1.0 **POLICY STATEMENT**

1.1 Dyfed-Powys Police processes personal data and has a duty to notify (register) with the Information Commissioner. The Registration Number Z489524X is recorded in the Information Commissioner Register of data controllers in order to use and disclose personal data which is governed in the United Kingdom by the Data Protection Act 1998. (please refer to Appendix A)

1.2 The Chief Constable is the Data Controller for Dyfed-Powys Police (DPP). Management of the statutory obligations and the force data protection policy is delegated to the Force Data Protection Officer.

1.3 The overarching purpose for which the Police are registered with the Information Commissioner is that it allows Dyfed-Powys Police to obtain, hold, retain and process personal data as well as the prevention, detection of crime, apprehension, prosecution of offenders, maintenance of law and order, protection of life and property, vetting and licensing, public safety and rendering assistance to members of the public in accordance with force policy.

1.4 In addition to the 'policing' purpose Dyfed-Powys Police are also registered for the support purposes of (1) staff administration which covers appointments or removals, pay, discipline, superannuation, work management or other personnel matters in relation to staff and (2) administration and ancillary support for policing purpose which includes records of computer transactions / computer message logs, telephone message logs, police property management logs, etc.

1.5 Dyfed-Powys Police has a legal obligation to comply with the Data Protection Act 1998, the Computer Misuse Act 1990, the Freedom of Information Act 2000, the Copyright Designs and Patents Act 1998 and the Human Rights Act 1998. As well as ensuring compliance with the ACPO Manual for Data Protection Management, ACPO Community Security Policy and the Police National Computer System Security Policy and the Guidelines for the Management of Police Information.

1.6 Exchange of information is an essential ingredient in our quest to achieve our objectives. We will therefore, where appropriate and in line with legislation, disclose or exchange personal information with other agencies, organisations or persons. To achieve this, it is necessary that Information Sharing Agreements are written, so that both organisations are fully aware and sign up to the sharing of information, and that this sharing complies with the Data Protection Act 1998.

1.7 In the exercise of any power, authority or directive under this policy, each member of staff must:

(a) give due regards to the privacy and human rights of all individuals;

(b) make full use of all current and relevant legislation;

(c) not unjustifiably discriminate against any individual or group of individuals;

(d) ensure that each action taken is justified and strictly proportionate to and is the least intrusive and damaging option required to secure the achievement of the legitimate aims.

1.8 That in the carrying out of this duty, it will be the duty of staff to follow a clearly defined decision making process by detailing their objectives, assessing all available and relevant information and options, documenting decisions made and reviewing outcomes.

1.9 This decision making process will be the subject of review and scrutiny by supervisors, managers and other parties as appropriate.

1.10 This policy is aimed at every member of Dyfed-Powys personnel whether employed, contracted or a volunteer including those external to Dyfed-Powys Police who have access to our information / systems and the communities of Dyfed-Powys Police.

1.11 Dyfed Powys Police is committed to protecting the rights of individuals with regard to the processing of personal data. Consequently the unlawful access and disclosure of information and the unauthorised holding or processing of personal data on police or privately owned computers will be considered to be serious misconduct. It has established the following policy to support this commitment.

1.12 The Force undertakes to apply this policy to all police officers, police staff, special constables, police volunteers and contractors.

1.13 Individuals working within the police service occupy a privileged position and 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 police officers and police staff who are 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.

1.14 This guideline is in keeping with the ACPO Code of Practice for Police Computer Systems and the Data Protection Act 1998. The day-to-day management of such matters will rest with the Data Protection Office at Headquarters where there is a 'HELP' line whenever assistance or advice is required on ext 23441 and 23447.

1.15 This guideline should also be read in conjunction with the Data Protection site on the Force Intranet.

2.0 INTRODUCTION

2.1 In order to achieve the lawful handling of personal data, the aim of Dyfed-Powys Police will be to comply with the eight Data Protection principles:

Principle 1

- data shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met;

Principle 2

- data shall be obtained only for one or more specified and lawful purpose, and shall not be further processed in any manner incompatible with that purpose or those purposes;

Principle 3

- data shall be adequate, relevant and not excessive in relation to the purpose of purposes for which they are processed;

Principle 4

- data shall be accurate and, where necessary, kept up to date;

Principle 5

- data shall not be kept for longer than necessary for that purpose or those purposes;

Principle 6

- data shall be processed in accordance with the rights of data subjects under the act.

Principle 7

- appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of , or damage to personal data;

Principle 8

- data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensure an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

2.2 Dyfed-Powys Police needs to collect, use and process types of information about the people with whom it deals in order to perform effectively as a police Force. These include current, past and prospective members of staff, offenders, victims, witnesses, suppliers, clients / customers and others with whom it communicates. This personal information must be dealt with properly when it is collected, recorded, used and destroyed, whether by manual or electronic means. DPP regard the lawful and correct treatment of personal information as important to the successful operation of the Force, achievement of our aims and objectives and to maintaining the confidence of members of the public. Numerous recording systems exist within the organisation and the integrity and value of this information is

paramount. The communities served by Dyfed-Powys Police expect data to be treated in line with legislation. If any breach of the Data Protection Act 1998 occurs then this will be recorded on a spreadsheet and reported to the Information Commissioners Office. This spreadsheet will be maintained by the Information Management Department

2.3 Dyfed-Powys Police will ensure access is provided for individuals who are lawfully entitled to request disclosure of personal information in accordance with Section 7 of the Data Protection Act 1998.

2.4 The legal basis for the exercise of any power, authority or directive under this policy is:

- Data Protection Act 1998
- Crime & Disorder Act 1998
- Police Act 1996
- Police Act 1997
- Police and Criminal Evidence Act 1984
- Rehabilitation of Offenders Act 1974
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Code of Practice on the Management of Police Information 2005
- ACPO Data Protection Manual of Guidance
- PNC National Operating Rules
- Dyfed-Powys Information Security Policy and Information Technology Strategy
- The National Strategy for Police Information Systems including the Police Community Security Policy

2.5 Dyfed-Powys Police consider that any action taken under this policy is necessary in a democratic society in the interests of:

- National security
- Public safety
- Economic well-being of the country
- Prevention of crime and disorder
- Protection of health and morals
- Preventing the disclosure of information received in confidence
- Protection of the reputations, rights and freedom of others

2.6 The Data Protection Act 1998 ('the Act') regulates the use of information from which a living individual can be identified (i.e. personal data) and creates a number of roles namely:

a. Information Commissioner - appointed by the Crown to supervise the legislation contained in the Data Protection Act 1998.

b. Data Controller - A person who determines the purposes for which and the

manner in which any personal data are processed. The data controller for the Dyfed Powys Constabulary is the Chief Constable.

c. Data Subject - an individual who is the subject of personal data.

2.7 The Act also establishes a Data Protection Tribunal, which provides machinery for appeals by data users against decisions made by the Commissioner.

3.0 DEFINITION OF TERMS AND PROCEDURES

3.1 The Data Protection Office will:

a) Ensure that guidance is available on all matters of the Act.

b) Ensure the Information Commissioner is notified of the processing of personal data.

c) Ensure the Information Commissioner is notified should a breach of Data Protection occur

d) Deal with all matters relating to subject access.

e) Audit the Force to ensure compliance with the Act.

3.2 Data Controller – means a person who determines the purpose for which and the manner in which any personal data are, or are to be, processed.

3.3 Personal Data – means data which relates to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of the data controller.

It includes expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

4.0 REPORTING OF DATA PROTECTION BREACHES

4.1 Any police officer or staff member, who becomes aware of a potential breach of the Act 1998 should immediately notify the Force Data Protection Manager on Extension 23441 or by e-mailing dataprotection@dyfed-powys.pnn.police.uk.

4.2 All Force information relating to identifiable individuals is personal data. Some personal data is classed as sensitive and more restrictions apply when there is a need to process sensitive data. Access and use of such information by police Officers, Police Staff and Special Constables must only be in the course of their official duties. This includes police volunteers under the Dyfed Powys Constabulary volunteer programme or any other approved person carrying out voluntary activity on behalf of the Force. Use for any other purpose is prohibited and may result in criminal and disciplinary proceedings.

4.3 This policy also relates to access and appropriate use of Share Point and other systems available to the Force. This includes data auditing processes which are relevant to the correct usage of the system. Access to the Share Point database is closely monitored by the Force.

4.4 Access to any Force IT equipment must be controlled. Only authorised operators in the course of official police business should have access.

4.5 Where a police officer or staff member is involved in or witnesses a crime or incident whilst off duty, no access to the recorded information can be made without prior authorisation from their line manager.

4.6 Deliberate unauthorised access to, copying, destruction or alteration of, or interference with any computer or ancillary equipment or data is strictly forbidden.

4.7 Under Section 55 of the Data Protection Act 1998 concerns the misuse of police held personal data by those working for or on behalf of a police force. It is **NOT** acceptable for a member of the Force to conduct checks on:

a. Nominals living in close proximity to them which include members of family and friends;

b. Friends or friends of family members;

c. Prospective employees of members of friends or family;

d. Individuals applying for membership of social and or other clubs;

e. The desirability of property;

f. Individuals subject to enquiries by private detective agencies.

This is not an exhaustive list. If in doubt, advice should be sought.

4.8 It is recognised that members of the Force (police officers, police staff and special constabulary) may have contact whilst off-duty, through family or social relationships, with people who are, or may be, of interest to the police or parties who have been involved with the police as victims or offenders. As a result of information that they become aware of directly or indirectly members of the Force

may consider it necessary to take further action.

4.9 In the interests of the integrity of the Force and the individual, where it is felt necessary to access the Force information, members of the Force will inform their line manager / supervisor. If the line manager / supervisor is not available, they should contact another supervisor. The line manager will, if appropriate, access Force information. A record will be made of this access and its justification. In the case of police officers and special constables this will noted on their tablets. In cases of doubt, before accessing Force information, the line manager should seek guidance from the Anti-Corruption and Intelligence Unit (ext. 23581) or Data Protection Office (ext. 23441 and 23447). The line manager / supervisor must be satisfied that the check is being undertaken for official police purposes.

4.10 Such contacts are potentially valuable sources of information and should not be discouraged. However, staff should be aware of the risk that their actions could be misinterpreted and should take the steps recommended above to allay any challenge to their integrity.

5.0 MISCONDUCT / CRIMINAL INVESTIGATIONS

5.1 Where an alleged breach of "the Act" results in a misconduct, discipline or criminal investigation being undertaken, the Head of the Professional Standards Department must assess the individual circumstances and ensure that the Force Data Protection Manager is notified within an appropriate time period.

5.2 This should be undertaken to ensure the safeguarding of information and early containment and recovery of any information and early preventative intervention to mitigate the risk of a similar circumstance occurring again.

5.3 The Force Data Protection Manager will conduct daily transaction audit to monitor compliance with , "the Act". ACPO Part 2 of the Manual of Guidance outlines the conduct of daily transaction audits #TE PNC audit.

6.0 INTERNAL INVESTIGATION – ROLES RESPONSIBILITIES AND THE ESCALATION PROCESS

6.1 Following the reporting of an alleged breach of data protection, the Data Protection Manager will gather information concerning the nature and context of the alleged breach. An assessment will be made using the matrix "Appendix A". A report covering the circumstances, will be created within 48 hours.

6.2 Should a breach of "the Act" have occurred and the breach is to be referred to the ICO, a record will be entered onto the Data Protection Breach spreadsheet: a proportionate investigation will be conducted to:

- establish if a breach has occurred;
- contain and recover any material;
- notify any individuals or organisations impacted by the breach;
- evaluate and respond to the breach ensuring any lessons learnt are fed back to the business area and wider organisation;
- submit a report to the Force Learning the Lessons Group;
- Data Protection Spreadsheet to be updated accordingly

6.3 In undertaking the above, full cognisance will be taken of the Information Commissioner's Guidance, which can be found at the following links:

http://www.ico.org.uk/for organisations/data protection/~/media/documents/library/data protection/practical application/guidance on data security breach management.ashx

http://www.ico.org.uk/for organisations/data protection/the guide/~/media/documents/library/data protection/practical application/breach reporting.ashx

6.4 The Information Assurance Board provides the strategic governance for Data Protection matters and local investigations and any breaches reported to the ICO will be reported to the Board.

6.5 The IA Board's role is to maintain oversight of DP issues, ensuring that appropriate investigation, action and lessons are learnt following on from any breach.

6.6 Where a breach involves referral to the ICO and / or the loss of a significant amount of personal data, a sub group of the IA Board will be formed.

6.7 The group will be made up of the DCC (Chair), Force Data Protection Manager and Force Information Security Officer and any other person who can add value to the group in their role of fully evaluating the breach, establishing the lessons to be learnt and ensuring ownership of relevant actions in respect of future prevention, recovery and containment.

6.8 The sub group will be formed at the recommendation of the IA Board

6.9 Disclosure of information may take many forms, including viewing records on terminals, computer printouts, typewritten material (which includes information taken from computer records) by word of mouth or radio transmission.

7.0 THIRD PARTY DISCLOSURE PROCESSES

7.1 Information will only be disclosed once an operator is fully satisfied that the enquirer or recipient is authorised in all respects and is legally entitled. This may involve deferring the enquirer until verification is sought, adopting 'call back' procedures or advising the enquirer to apply in writing, to the Data Protection Office. The identity of the subject of the enquiry must be satisfactorily established. Any unauthorised disclosure held in any form by or on behalf of the Force may render the officer or police staff employee liable to criminal and disciplinary proceedings.

7.2 The Force works with a number of partner agencies to jointly tackle issues relating to crime and anti social behaviour. Information exchange protocols provide the legal and procedural framework for disclosure.

7.3 It should also be noted that circumstances might arise when it is in the public interest for limited personal information to be released into the public domain. For example; where advice is sought by member of the public concerning the risks that may be posed to a third party, such as children, or to the community in general, by an individual. This is NOT a decision that can be made by any individual member of staff who receives such an enquiry. The Multi Agency Public Protection Panels are set up as a forum to assess and manage the risks posed by certain dangerous offenders.

7.4 When enquiries of this nature are received from members of the public, the following procedure should be followed; a Protect Log should be created and referred to the appropriate Child Abuse Investigation Unit via the Central Referral Unit. This course of action will be in slow time, however, if it is perceived that there is an immediate risk then the relevant log should be brought to the attention of the BCU Commander or your line manager. The Data Protection and Human Rights of an individual must be balanced against the risk posed to a person and / or the community. Provided there is no immediate risk to any person the matter can be dealt with by the PVP Officer, with the aid of the Director of Force Intelligence to Assistant Chief Constable for a decision to be made.

7.5 Staff should be aware that staff information can be disclosed under the Freedom Of Information Act 2000. Please refer to the guidance found in the Freedom of Information Force Policy.

7.6 In case of doubt concerning information disclosure, advice may be sought from:

Data Protection Office ext. 23441

Head of Information Management ext. 23175

7.7 The Data Protection Officer is responsible for notifying the Information Commissioner of the processing of personal data. Copies of the notification are available from the office on request.

8.0 CONSEQUENCES OF NON-COMPLIANCE

8.1 "the Act" 1998 grants extensive power to the Information Commissioner and provides more extensive rights for the individual. An individual has the right to claim compensation for damage or distress suffered as a result of non-compliance, be it inappropriate processing or poor data quality. If an individual complains to the Office of the Information Commissioner then the Information Commissioner is obliged to investigate to establish if a breach of "the Act" has occurred.

8.2 **Enforcement**

The Commissioner can serve a Data Controller with an 'information notice' requiring the Data Controller to provide certain information within set time limits. Failure to comply with such a notice, or providing deliberately false information, is a criminal offence.

8.3 If the Commissioner concludes that there has been a breach of the Act he may then serve a Data Controller with an 'enforcement notice'. This could force a Data Controller to cease processing personal data, or cease processing data in a particular way which could be catastrophic for the Force. Failure to comply with an enforcement notice is a criminal offence.

8.4 The unauthorised holding or processing of personal data on police or privately owned computers can result in criminal prosecution and disciplinary proceedings, therefore all unauthorised processing of personal data on police equipment is prohibited.

8.5 Additionally, the use of privately owned computers or word processors for police purposes is prohibited for Sensitive Information, including information which is considered CLOSED (under FOI) at the time of creation.

8.6 Limited home working for business or operational reasons is permitted only in accordance with paragraph 4.4 and 8.4 and

a. after authorisation from your BCU Commander or Departmental Manager

b. the information is not protectively marked see Force Information Assurance Government Protective Marking Scheme Working Practice document

c. the information is not CLOSED under FOI

8.7 The PNC and Force computer systems, including word processors, are intended solely for official policing purposes and must be used only where the member of staff duties specifically warrant this. Use for any other purpose is prohibited and may render the officer or police staff employee liable to criminal and disciplinary proceedings.

8.8 Personal data held on electronic diaries and organisers are subject to the provisions of "the Act". Individually owned computers of this type may not be used to hold intelligence information. Refer to Force Information Security Policy.

8.9 Under no circumstance will non Dyfed Powys Police computer disks or media containing data be installed onto any Force IT Equipment until they have been checked for computer viruses and other forms or malicious software.

8.10 Under no circumstance will computer disks or media containing software be installed onto any Force IT Equipment. All software requests should be directed through the local IS & T Department.

9.0 CRIMINAL OFFENCES

9.1 A number of criminal offences are created by "the Act". The data controller is guilty of an offence if they

(a) are processing without notification;

(b) fail to notify the Commissioner of changes to notification register entry;

(c) fail to comply with written request for particulars;

(d) fail to comply with an enforcement notice / information notice / special information notice;

(e) knowingly or recklessly make a false statement in compliance with an enforcement notice or special information notice;

(f) Intentionally obstructs, or fails to give reasonable assistance in the execution of a warrant.

9.2 However, it is not just the Data Controller who is criminally liable. Police Officers and police Staff in Dyfed Powys Police are considered to be servants or agents of the Chief Constable (the Data Controller) and as such can be personally criminally liable if they disclose or obtain personal data without the authority of the Data Controller. Therefore, if you make, or encourage another person to make an unauthorised disclosure knowingly or recklessly you may be held criminally liable.

9.3 The offences that apply are given at Section 55 of the Act and are as follows:

(a) without the consent of the Chief Constable (Data Controller), knowingly or recklessly to unlawfully obtain or disclose personal data or the information contained in personal data; or procure the disclosure to another person of the information contained in personal data;

(b) without the consent of the Chief Constable (Data Controller) to knowingly or recklessly procure the disclosure to another person of the information contained in personal data;

(c) There is another offence committed by a person selling personal data if it has been obtained in contravention of the above or offers to sell information obtained or to be obtained in contravention of the above.

9.4 This does not apply if it can be shown:

(i) that the obtaining, disclosing or procuring –

- was necessary for the purpose of preventing or detecting crime;

OR

- was required or authorised by or under any enactment, by any rule of law or by the order of a court;

(ii) that an individual acted in the reasonable belief that they had in law the right to obtain or disclose the data or to procure the disclosure to another person;

(iii) that they acted in the reasonable belief that the Chief Constable would have consented if they had known of the obtaining, disclosing or procuring and the circumstances of it; "or"

(iv) that in the particular circumstances the obtaining, disclosing or procuring was justified as being in the public interest.

9.5 In addition, in respect of computer processed information, the following activities are criminal offences under the Computer Misuse Act 1990:

- unauthorised access to computer material;
- unauthorised modification of computer material, and
- unauthorised access with intent to commit / facilitate the commission of further offences.

10.0 SUBJECT ACCESS

10.1 "the Act" 1998 provides that subject to certain provisions, an individual shall be entitled:

(a) to be informed by the Data Controller whether data held includes personal data of which that individual is the subject; and

(b) to be supplied by the Data Controller with a copy of the information constituting any such personal data held by him.

10.2 A time limit of forty days is specified by the Act to reply to such requests. The Force will comply with the requirements of "the Act" in respect of Subject Access to information held by Dyfed-Powys Police. Subject Access requests will only be processed though the Data Protection Unit.

10.3 The ACPO Code of Practice for data protection is available on the Data Protection site on the Force Intranet.

11.0 DEROGATIONS

Nil.

12.0 ENFORCEMENT AND REPORTING

12.1 All staff, in particular managers and supervisors, will be responsible for the implementation and operation of this policy.

13.0 PUBLIC ACCESS TO COMPUTERS

13.1 All terminals must be sited so that data displayed is kept from public view at all times. Visitors must not be allowed to view 'live' information and no 'real' transaction should be carried out in their presence.

13.2 Logged on terminals are to be continuously manned or locked when not in use. At no time will data be displayed on an unattended or unsupervised VDU screen.

14.0 SECURITY

14.1 Access to any computer working area must be restricted to authorised operators or to any other personnel in the course of their official duty.

14.2 The use or disclosure of another person's 'log on' or password is strictly forbidden.

14.3 Where technically possible, a password protection system must be used. Guidance on password composition and use can be found in Force Information Security Policy.

14.4 Manufacturers or maintenance staff attending to repair computer equipment will not, unless unavoidable, be allowed to view live data. Such persons should not be allowed access to a terminal unaccompanied. If maintenance staff require access to 'live' data, IS & T Department will be advised prior to access for verification that such access is necessary.

15.0 ACCURACY OF DATA

15.1 It is the responsibility of those who receive information to ensure, so far as is possible, that it is accurate, valid and up-to-date.

15.2 Those causing information to be entered on police records must ensure that it is adequate, relevant, unambiguous and professionally worded. All staff should be made aware that information may be disclosed to the subject (see Section 17). If an operator discovers or suspects that personal data is inaccurate, the operator will immediately contact the source of the information and rectify the inaccuracy. If doubt exists, the data must be removed and the matter reported to the user departmental systems manager.

15.3 The source of data when reviewed from a data subject or from a third party must be recorded accurately. Notations of this nature will safeguard the data user in the event of the information proving to be inaccurate.

15.4 Matters of opinion, not fact, must be clearly recorded as such.

16.0 MANUAL DATA/TAPE FOOTAGE

16.1 All personal data are subject to data protection legislation. It is therefore essential that care is exercised with regard to the movement, storage and disposal of any manual data or tape footage. Under normal circumstances personal data should be NOT

17.0 REVIEW AND REMOVAL OF DATA

17.1 Unless a system incorporates automatic weeding facilities, reviews of personal data must be carried out at frequent intervals to ensure immediate cancellation or amendment of unwanted or out-of-date material. See Mopi Policy Records Management.

17.2 All print-out material, magnetic tape, diskettes, etc. no longer required will be disposed of according to Force Information Assurance Government Protective Marking Working Practice Document. Disposal will depend on the protective marking of the information or material.

18.0 SUBJECT ACCESS PROCESS

18.1 Individuals have a right of access to personal data held about them. Information will be provided in accordance with these procedures.

18.2 There is no obligation to supply information unless the request is made in writing, the prescribed fee is paid and sufficient information is given to trace the data. All subject access enquiries should be referred to the Data Protection Office without delay.

18.3 Form SA1 is used by the Data Protection Office to assist in the processing of subject access requests. Persons making enquiries about how to apply for subject access must be referred to the Data Protection Office ext. 23441.

18.4 Initial enquiries received by post should be checked and matters not connected with data protection dealt with. If the letter is a request for an application form or touches upon any other data protection issue, it must be forwarded to the Data Protection Office, Force Headquarters, Llangunnor, Carmarthen by internal post.

18.5 The procedure for processing application forms is as follows:

a) Check that the form is complete and legible.

b) Verify the identity of the applicant. Return the ID documents to the applicant.

c) Collect the fee of £10.00 and issue a police account receipt.

d) Enter the information onto the Subject Access Database

e) Send out the letter that it generates to the applicant

f) Open a file stating the start and expected date of dispatch

g) Research Information Assets for the requested information

h) Save the information and give the file the number name

i) Copy all the research and paste under the research information (this is the information you will be redacting)

j) Redact the information in line with "the Act"

k) Disclose information by next day delivery

l) Retention of Subject Access is 2 years

19.0 NON-DISCLOSURE EXEMPTION

19.1 Principle 2 of "the Act" states that 'personal data shall be processed for limited and lawful purposes'.

19.2 The Act contains certain exemptions which permit the disclosure of personal data when necessary for:

a) National security: disclosure for the purpose of safeguarding national security;

b) Prevention or detection of crime, the apprehension or prosecution of offenders, only where the application of those provisions in relation to the disclosure would be likely to cause serious prejudice;

c) The assessment of collection of any tax or duty, only where the application of those provisions in relation to the disclosure would be likely to cause serious prejudice;

d) Disclosure required by enactment, by any law or by order of a court;

e) Disclosure for the purpose of obtaining legal advice or in connection with any legal proceedings;

f) In the following cases:

(i) Disclosure to the data subject or to a person acting on their behalf;

(ii) Disclosure at the request or with the consent of the data subject;

(iii) Disclosure by the chief officer to their servant or agent;

(iv) Reasonable belief that (1), (2) or (3) apply.

g) Disclosure urgently required to protect the vital interests of any person or persons.

19.3 The decision to use a non-disclosure exemption MUST be made on a CASE BY CASE basis.

19.4 Instances may arise when a police officer requires personal data from another organisation using the non-disclosure exemption as at 16.2(b) above. Should this occur, the organisation should be served with a Section 29 Form. In exceptional circumstances, because of the nature of the investigation or because of its sensitivity, it may not be possible for all details on the Section 29 Form to be provided. When this occurs, the form should be countersigned by an officer of the rank of superintendent or above. Section 29 Form can be found on the Data Protection site on the Force Intranet.

19.5 If a request is made for information using a non- disclosure exemption and there are no reasonable grounds for using the exemption, then the request is unlawful and a criminal offence may be committed (section 55 (1) (3) of "the Act" 1998).

20.0 DATA PROTECTION ACT OFFENCES

20.1 The ACPO Manual of Guidance on Data Protection for the Police Service sets out, within section 9, the procedures for the recording and handling of allegations of criminal offences committed in contravention of "the Act". It describes the role of the police and the Information Commissioner and the actions to be taken when criminal offences under the Act are suspected.

21.0 COPYRIGHT, DESIGNS AND PATENTS ACT 1988

21.1 Under the Act, the owner of the copyright has the exclusive right to copy the work. It is therefore illegal both to copy software without the copyright owner's permission and to use such unauthorised software.

22.0 THE MAKING, ACQUISITION OR USE OF UNAUTHORISED COPIES OF COMPUTER SOFTWARE WITHIN THE FORCE IS PROHIBITED

22.1 If software is required, ensure that properly licensed software is obtained, contact the IS & T Department.

23.0 AUDIT DECLARATION

23.1 This policy has been drafted and audited in accordance with the principles of Human Rights Legislation, the Race Relations (Amendment) Act 2000, Disability Discrimination Act 1995, the Policing Bureaucracy Gateway and Freedom of Information Act 2000. Under the Freedom of Information Act 2000, the document is classified as 'OPEN'.

24.0 REVIEW

24.1 The biannual review of this policy is the responsibility of Head of Information Management.

25. ACCESSIBILITY, REDRESS AND REVIEWS

25.1 This policy will be published and made readily available to all police officers and police staff via the Force Intranet System.

25.2 This policy is a public document and will be made available to the general public via the Force Publication Scheme – www.dyfedpowys.police.uk - and upon written request to the Inforamtion Management Unit.

25.3 This policy will be reviewed biannually by the Data ProtectionManager and verified by Legal Services to ensure compliance with Human Rights, other legislation and guidance documents. There will also be subject to audit by Her Majesty's Inspector of Constabularies (HMIC). The policy will be published in a format making it easily readable.

25.4 Any person(s) who has / have cause to feel aggrieved by any matter outlined in this policy is / are able to and may seek redress in the following ways:

- Misconduct procedures
- Civil or criminal proceedings
- Direction and control procedure
- Reconciliation procedure

25.5 Any person in exercising their right, as detailed in paragraph 24.4 above, will have the right of equal access to information and the right to seek legal advice.

25.6 Public consultation is an important part of this process, with views and comments welcomed. These should be addressed to the

Chief Constable,
Dyfed-Powys Police Service,
PO Box 99,
Llangunnor,
CARMARTHEN,
Carmarthenshire. SA31 2PF

Signed: Date: 01st September 2017

Darren Davies
Deputy Chief Constable

Records created as a result of Force Policy - Data Protection **Paragraph**	**Type of record**	**Where held**	**Retention Period**
5.3	Audit records PNC transactions	Data Protection Office	Personal data 3 months. Statistical data indefinitely.
18.3	Subject access application files	Data Protection Office	2 years for access to Force systems. 1 year for access to PNC.

A new Data Protection APP is now available for an indepth understanding of The Data Protection Act 1998 https://www.app.college.police.uk/app-content/information-management/data-protection/

APPENDIX A

NOT PROTECTIVELY MARKED

How we use Personal Information

Introduction

This document explains how the Dyfed Powys Police Forceobtains, holds, uses and discloses information about people - their personal information[1] -, the steps we take to ensure that it is protected, and also describes the rights individuals have in regard to their personal information handled by the Constabulary[2].

The use and disclosure of personal information is governed in the United Kingdom by the Data Protection Act 1998 ('the Act'). The Chief Constable is registered with the Information Commissioner as a 'data controller' for the purposes of the Act. As such he is obliged to ensure that the Constabulary handles all personal information in accordance with the Act. The registration number is Z489524X

The Constabulary takes that responsibility very seriously and takes great care to ensure that personal information is handled appropriately in order to secure and maintain individuals' trust and confidence in the force.

1. Why do we handle personal information?

The Force obtains, holds, uses and discloses personal information for two broad purposes:
1. The Policing Purpose – which includes the prevention and detection of crime; apprehension and prosecution of offenders; protecting life and property; preserving order; maintenance of law and order; rendering assistance to the public in accordance with force policies and procedures; and any duty or responsibility of the police arising from common or statute law.

1 'Personal Data' is defined under Section 1 of the Data Protection Act 1998. In practical terms it means information handled by The Constabulary that relates to identifiable living individuals. It can include intentions and expressions of opinion about the individual. The information can be held electronically or as part of paper records, and can include CCTV footage and photographs. For ease of readers this
document refers to the handling, use, holding etc of personal data – Section 1 of the Act uses the term 'processes' to effectively cover any usage of personal data.
2 This document is designed to help satisfy the 'Fair Processing Requirements' as required by Schedule 1 Part 2 Paragraphs 1 to 4 of the Data Protection Act 1998 and may be regarded as a generic over-arching 'Fair Processing Notice' for The Constabulary. Additional more specific Fair Processing Notices may appear in other circumstances such as on forms, force policies, email footers, or CCTV signage
.

2. The provision of services to support the Policing Purpose – which include:

- Staff administration,
- Occupational health and welfare;
- Management of public relations, journalism, advertising and media;
- Management of finance;
- Internal review, accounting and auditing;
- Training;
- Property management;
- Insurance management;
- Vehicle and transport management;
- Payroll and benefits management;
- Management of complaints;
- Vetting;
- Management of information technology systems;
- Legal services;
- Information provision;
- Licensing and registration;
- Pensioner administration;
- Research, including surveys[3];
- Performance management;
- Sports and recreation;
- Procurement;
- Planning;
- System testing;
- Security;
- Health and safety management

2. Whose personal information do we handle?

In order to carry out the purposes described under section 1 above the Force may obtain, use and disclose (see section 7 below) personal information relating to a wide variety of individuals including the following:

- Staff including volunteers, agents, temporary and casual workers;
- Suppliers;
- Complainants, correspondents and enquirers;
- Relatives, guardians and associates of the individual concerned;
- Advisers, consultants and other professional experts;
- Offenders and suspected offenders;
- Witnesses;
- Victims;
- Former and potential members of staff, pensioners and beneficiaries;
- Other individuals necessarily identified in the course of police enquiries and activity.

The Force will only use appropriate personal information necessary to fulfil a particular purpose or purposes.

Personal information could be information which is held on a computer, in a paper record such as a file, as images, but it can also include other types of electronically held information such as CCTV images.

3 The Constabulary is required to conduct Customer Satisfaction Surveys to evaluate our performance and effectiveness. We may contact individuals, such as victims of crime or those reporting incidents, and ask them to give us their opinion of the service we are providing to the public. We use the information given to improve our service wherever we can. The Constabulary, like many police forces uses a private company to undertake such surveys on our behalf with strict controls to protect the personal data of those involved.

3. What types of personal information do we handle?

In order to carry out the purposes described under section 1 above, the Force may obtain, use and disclose (see section 7 below) personal information relating to or consisting of the following:

- Personal details such as name, address and biographical details;
- Family, lifestyle and social circumstances;
- Education and training details;
- Employment details;
- Financial details;
- Goods or services provided;
- Racial or ethnic origin;
- Political opinions;
- Religious or other beliefs of a similar nature;
- Trade union membership;
- Physical or mental health or condition;
- Sexual life;
- Offences (including alleged offences);
- Criminal proceedings, outcomes and sentences;
- Physical identifiers including DNA, fingerprints and other genetic samples;
- Sound and visual images;
- Licenses or permits held;
- Criminal Intelligence;
- References to manual records or files;
- Information relating to health and safety;
- Complaint, incident and accident details.

4. Where do we obtain personal information from?

In order to carry out the purposes described under section 1 above the Force may obtain personal information from a wide variety of sources, including the following:

- Other law enforcement agencies;
- HM Revenue and Customs;
- International law enforcement agencies and bodies;
- Licensing authorities;
- Legal representatives;
- Prosecuting authorities;
- Defence solicitors;
- Courts;
- Prisons;
- Security companies;
- Partner agencies involved in crime and disorder strategies;
- Private sector organisations working with the police in anti-crime strategies;
- Voluntary sector organisations;
- Approved organisations and people working with the police;

- Independent Police Complaints Commission;
- Her Majesty's Inspectorate of Constabulary;
- Auditors;
- Police Authority;
- Central government, governmental agencies and departments;
- Emergency services;
- Individuals themselves;
- Relatives, guardians or other persons associated with the individual;
- Current, past or prospective employers of the individual;
- Healthcare, social and welfare advisers or practitioners;
- Education, training establishments and examining bodies;
- Business associates and other professional advisors;
- Employees and agents of The Constabulary;
- Suppliers, providers of goods or services;
- Persons making an enquiry or complaint;
- Financial organisations and advisors;
- Credit reference agencies;
- Survey and research organisations;
- Trade, employer associations and professional bodies;
- Local government;
- Voluntary and charitable organisations;
- Ombudsmen and regulatory authorities;
- The media;
- Data Processors working on behalf of The Constabulary.
- The Constabulary may also obtain personal information from other sources such as its ownCCTV systems, or correspondence.

5. How do we handle personal information?

In order to achieve the purposes described under section 1 the Force will handle personal information in accordance with the Act. In particular we will ensure that personal information is handled fairly and lawfully with appropriate justification. We will strive to ensure that any personal information used by us or on our behalf is of the highest quality in terms of accuracy, relevance, adequacy and non-excessiveness, is kept as up-to-date as required, is protected appropriately, and is reviewed, retained and securely destroyed when no longer required. We will also respect individuals' rights under the Act (see section 8 below).

6. How do we ensure the security of personal information?

The Constabulary takes the security of all personal information under our control very seriously. We will comply with the relevant parts of the Act relating to security, and seek to comply with the Association of Chief Police Officers' Community Security Policy and relevant parts of the ISO27001/2 Information Security Standard.

We will ensure that appropriate policy, training, technical and procedural measures are in place, including audit and inspection, to protect our manual and electronic information systems from data loss and misuse, and only permit access to them when there is a legitimate reason to do so, and then under strict guidelines as to what use may be made of any personal information contained within them. These procedures are continuously managed and enhanced to ensure up-to-date security.

7. Who do we disclose personal information to?

In order to carry out the purposes described under section 1 above the Force may disclose personal information to a wide variety of recipients in any part of the world, including those from whom personal information is obtained (as listed above). This may include disclosures to other law enforcement agencies, partner agencies working on crime reduction initiatives, partners in the Criminal Justice arena, Victim Support, and to bodies or individuals working on our behalf such as IT contractors or survey organisations. We may also disclose to other bodies or individuals where necessary to prevent harm to individuals. Where required, or appropriate to do so, personal data may be shared with the Office of the Police and Crime Commissioner (including the Commissioner, its staff, agents or appointed volunteers) to facilitate and support policing and to deliver applicable statutory functions. Disclosures of personal information will be made on a case-by-case basis, using the personal information appropriate to a specific purpose and circumstance, and with necessary controls in place. Some of the bodies or individuals to which we may disclose personal information are situated outside of the European Union - some of which do not have laws that protect data protection rights as extensively as in the United Kingdom. If we do transfer personal information to such territories, we will take proper steps to ensure that it is adequately protected as required by the Act.

The Force will also disclose personal information to other bodies or individuals when required to do so by, or under, any act of legislation, by any rule of law, and by court order. This may include disclosures to the Child Support Agency, the National Fraud Initiative, the Home Office and to the Courts. The Constabulary may also disclose personal information on a discretionary basis for the purpose of, and in connection with, any legal proceedings or for obtaining legal advice.

8. What are the rights of the individuals whose personal information is handled by the Constabulary?

Individuals have various rights enshrined in the Act:

Subject Access

The most commonly exercised right is that used by individuals to obtain a copy, subject to exemptions, of their personal information processed by the Force. Details of the application process, known as 'Subject Access' can be found from the force internet at: http://www.dyfed-powys.pnn.police.uk

Alternatively individuals may contact the Force Data Protection Unit (see section 11 below).

Right to prevent processing likely to cause damage or distress

Under Section 10 of the Act an individual is entitled, in limited circumstances, to write to the Constabulary requiring that we do not handle their personal information in a manner that was causing or would be likely to cause unwarranted substantial damage or substantial distress to themselves or another person.
Requests under Section 10 must describe the personal information involved; describe the handling to which the individual objects; state that the handling was causing or would be likely to cause substantial damage or substantial distress to him/her or another; describe the damage or distress; state that the damage or distress was/would be unwarranted; and give reasons why the handling was causing/would cause such distress and was/would be unwarranted.
All requests of this nature may be sent in writing to the Force Data Protection Officer (see section 11 below). It is worth noting that the Act includes certain provisions which may mean in a particular case that the Constabulary can continue to handle the personal information as intended despite the objection.

Right to Prevent Processing for the Purposes of Direct Marketing

Although the Constabulary does not engage in direct–marketing, under Section 11 of the Act and subject to certain exemptions, an individual has the right to request in writing that the Constabulary stops within a reasonable time, or does not start, using their personal information for direct marketing purposes. This includes the communication by any means (e.g. mail, email, telephone, door-to-door canvassing) of any advertising or marketing material directed at particular individuals.
Any requests under Section 11 may be sent to the Constabulary Data Protection Officer (see section 11 below).

Rights in relation to automated decision-taking

Although the Constabulary is unlikely to carry out any automated decision-taking that does not involve some human element, under Section 12 of the Act and subject to certain exemptions, an individual has the right to require that the Constabulary ensures that no decision that would significantly affect them is taken by the Constabulary or on its behalf purely using automated decision-making software. The right has to be exercised in writing. If there is a human element involved in the decision-making the right does not apply. Requests under Section 12 may be sent to the Constabulary Data Protection Officer (see section 11 below).

Right to take action for compensation if the individual suffers damage by any contravention of the Act by data controllers

Under Section 13 of the Act any individual who believes they have suffered damage or distress and damage as a result of any contravention of the requirements of the Act may be entitled to compensation from the Constabulary where the force is unable to prove that it had taken such care as was reasonable in all the circumstances to comply with the relevant requirement.

Any claim for compensation arising from this provision may be sent to the Legal Department, Dyfed Powys Police Head Quarters, POBox 99, Llangunnor, Carmarthen, CM31 2PF

Right to take action to rectify, block, erase or destroy inaccurate data

Under Section 14 of the Act an individual has the right to seek a court order for the rectification, blocking, erasure or destruction of their inaccurate personal information handled by the Constabulary. The right cannot be exercised directly to the Constabulary.

Right to request the Information Commissioner to assess a data controller's Processing

Under Section 42 of the Act any person can request the Information Commissioner to make an assessment if they believe that they are/have been adversely affected by the handling of personal information by the Constabulary. Such requests should be made direct to the Information Commissioner whose contact details can be found below. Generally if individuals have any concerns regarding the way their personal information is handled by the Constabulary or the quality (accuracy, relevance, non-excessiveness etc.) of their personal information they are encouraged to raise them with the Constabulary Data Protection Officer (see section 10 below).
The Information Commissioner is the independent regulator responsible for enforcing the Act and can provide useful information about the Act's requirements. The Information Commissioner's Office may be contacted using the following:
Mail: The Information Commissioner's Office,
Wycliffe House,
Wilmslow,
Cheshire,
SK9 5AF
Telephone: 01625 545700
Website: www.ico.gov.uk

9. How long does The Constabulary retain personal information?

The Constabulary keeps personal information as long as is necessary for the particular purpose or purposes for which it is held. In respect of the Police National Computer (PNC), personal information is retained, reviewed and deleted in accordance with agreed national retention periods which are subject to periodic change. Records containing personal information relating to intelligence, custody, crime, firearms, conviction history, child abuse investigations, and domestic violence will be retained in accordance with National Policy. The main one being the Guidance on the Management of Police Information (MoPI) 2010. This can also be found on the National Policing Improvement Agency (NPIA) website - http://www.npia.police.uk/en/15088.htm

For all other records not covered by the foregoing, the Force Record Retention Schedule applies.

10. Monitoring

The Constabulary may monitor or record and retain telephone calls, texts, emails and other electronic communications to and from the force in order to deter, prevent and detect inappropriate or criminal activity, to ensure security, and to assist the purposes described under section 1 above.

11. Contact Us

Any individual with concerns over the way the Constabulary handles their personal information
may contact our Data Protection Officer as below:
Telephone: 01267 222020
Email: dataprotection@dyfed-powys.pnn.police.uk
Mail: Data Protection Officer, Dyfed Powys Police, PO Box 99, Llangunnor, Carmarthen, SA31 2PF
Website: www.dyfed-powys.police.uk

NOT PROTECTIVELY MARKED
V1 3rd October 2017

Guidance from ACRO Criminal Records Office Data Protection Breach Policy and Standard Operating Procedure (not to be published)