Data Protection Procedure

This procedure is part of North Yorkshire Police policy to which all Chief Constable personnel and the functions provided by the Police and Crime Commissioner are required to adhere.

Procedure Statement

North Yorkshire Police (NYP) and the Police and Crime Commissioner for North Yorkshire (OPCC) are committed to ensuring that staff undertake their legitimate duties in a manner that is compatible with the data protection principles.

NYP and the OPCC recognise the sensitivity of processed personal information and its obligations in respect of data held by NYP/the OPCC i.e. to protect individuals from harm caused by the use of inaccurate information or the misuse of correct information.

NYP and the OPCC also acknowledge the clear benefits of having accurate and up-to-date information available for use in an appropriate format, when and where it is required. A pragmatic approach to the application of the principles within the Data Protection Act 1998 will help to deliver these benefits.

Overarching Policies:
Records Management Policy

Procedures:
Data Protection – Subject Access Procedure
Protective Marking Procedure (pre September 2016)
Protective Marking Procedure (from September 2016 onwards)
Review, Retention and Disposal of Information Procedure
Clear Desk and Clear Screen Procedure
Internet, Email and Mobile Phone Procedure
Information Security Policy
Freedom of Information Procedure
Management & Submission of Intelligence Information Procedure
National Intelligence Model (Daily) Procedure
Safeguarding Children from Abuse Procedure
Domestic Abuse Procedure
National Crime Recording Standard Procedure
National Standards for Incident Recording Procedure
Collection and Recording of Police Information (Niche RMS) Procedure
Data Protection Procedure

Process

Data Acts

The Data Protection Act is intended to protect the rights of individuals when information is processed about them by organisations including the police. The act is concerned with all personal information whether it is processed on computer, CCTV, manual filing records, microfiche, or any other media.

Types of Information

- de-personalised data is anonymised, sanitised or aggregated information which does not identify an individual in any way (including using other information available)
- personal data relates to a living individual who can be directly or indirectly identified from the data available, e.g. name, address, postcode, vehicle registration mark (VRM) etc
- sensitive personal data relates to an individual’s health, sexual life, racial or ethnic origin, religious beliefs, political opinion, any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings. This type of data would also include domestic abuse, rape and sexual assault information and police intelligence

The act sets out eight principles for good information, handling and processing, a full description of each can be found at the following link: Data Protection Act 1998 and within APP guidance

“Processing” under the act includes: Obtaining, recording, holding, organising, adapting, altering, retrieving, disclosing of the data by transmission / electronic means, dissemination, combining, blocking, erasure and destruction.

The principles are enforceable by the Information Commissioner and courts and a number of offences are established by the act. Misuse of personal information could result in a conviction and a fine. It is important that staff understand that they may be committing an offence if they misuse information and a more detailed explanation can be found within APP guidance under the heading Handling allegations of criminal offences under the Data Protection Act 1998

Legitimate Use

The principal purposes for which NYP processes information are:

- prevention and detection of crime
- apprehension and prosecution of offenders
- protection of life and property
- maintenance of law and order
- rendering assistance to the public in accordance with force policies and procedures

Data Protection Procedure
Information is also processed for specific purposes relating to the administration of NYP and its employees.

The principle purpose for which the OPCC processes information is to improve accountability within the police force and ensure that NYP is combating issues important to the community. Information is also processed for purposes relating to administration of the OPCC and its employees and the use of CCTV systems for crime prevention.

The Data Protection Act (DPA) 1998 applies to the processing of personal data contained within any electronic or paper based system. Examples are:

- computer records
- e-mail
- backup/archive systems
- word processing documents
- CCTV recordings
- audio/video recordings
- microfiche
- the majority of manual filing systems

**Request for Information**

Requests for the disclosure of any personal information will only be processed once the member of staff, whether a police officer or police staff, is fully satisfied that the enquirer or recipient is authorised to receive the information. Care must be taken to ensure that any disclosure has a lawful basis.

All police staff (including police officers) are prohibited from accessing personal data for any reason other than a policing purpose. Unauthorised access to data on police computers, including Police National Computer (PNC), known as 'browsing', is an offence under the Computer Misuse Act 1990. Additionally, a criminal offence under the DPA 1998 may be committed if the information is obtained, or used, in any way outside the notified purposes. Any unauthorised interrogation of police systems, or use of data held for a policing purpose, is likely to amount to a disciplinary offence. Public confidence in the security of data used for police purposes is of paramount importance.

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

To avoid any inadvertent unlawful disclosure, the use of ‘live’ data held on computer systems or in manual filing systems for training purposes is strictly prohibited without the express permission of the Police Lawyer (Civil Disclosure).

For further information on specific areas of disclosure, reference should be made to guidance such as:

- Crime and Disorder Protocols
- Pub and Shop Watch Protocols
Further advice and guidance concerning any aspect of civil disclosure may be obtained from the Civil Disclosure Unit at NYP Headquarters.

**Notification**

The national body for the supervision of data protection is the Information Commissioner to whom NYP and the OPCC notify the purposes for processing personal data. These notifications are subject to public scrutiny at main libraries and through the Office of the Information Commissioner’s website.

The Joint Corporate Legal Services Department is responsible for maintaining the notification process for both NYP and the OPCC. The principal purpose of notification is transparency and openness. It is a basic principle of the DPA 1998 that the public should know, or be able to find out, who is carrying out processing of personal data and for what purpose. A copy of the notifications are held at Legal Services at NYP Headquarters.

**Information Compliance**

The Civil Disclosure Unit has responsibilities for providing data protection advice and guidance within NYP and the OPCC, namely:

- ensuring that guidance is available on all aspects of the DPA 1998
- dealing with all matters relating to subject access
- providing data protection advice and guidance
- investigating and resolving complaints made concerning the use of data and where appropriate, assist in the investigation of disciplinary and criminal matters
- liaison between NYP, the ACPO Data Protection Portfolio Group and the Information Commissioner

**Information Security**

Principle Seven of the DPA 1998 requires NYP and the OPCC to ensure information is appropriately and adequately secured.

Information security refers to not only the physical or technical protective measures taken but also to procedural issues such as:

- Clear Desk and Clear Screen Procedure
- Internet, Email and Mobile Phone Procedure
- Protective Marking Procedure
- Information Security Policy

It is important that any Information Security breaches (including data breaches) are reported as detailed in the Security Incident Reporting Procedure. This information will then be passed to the

**Data Protection Procedure**
Police Lawyer (Civil Disclosure) who will assess the breach and the necessity to inform the Information Commissioners Office.

**Accuracy of Information**

It is the responsibility of the person who receives information to ensure, as far as is possible, that it is accurate, valid, and up-to-date.

When entering information onto a record (paper or IT based) staff must, as far as possible, ensure that it is adequate, relevant, unambiguous and professionally worded. Where errors are identified within any personal information held, they must be corrected at the earliest opportunity.

The source of data received from a data subject or a third party must be recorded accurately. These notes will assist an investigation, should the information or its source be challenged.

**Review and Removal of Information**

Unless a system incorporates automatic weeding facilities or other structured weeding procedures, reviews of personal data must be carried out at appropriate intervals to ensure cancellation or amendment of superfluous or out-of-date material. This is good practice that should be applied to all levels of information. The Review, Retention and Disposal of Information Procedure (NYP) and the Records Management & Correspondence Handling Procedure (OPCC) [hyperlink] should be referred to for further guidance.

**Confidential Waste**

All print-out material, magnetic tape, diskettes, manual files, hand-written notes etc, which contain personal data and are no longer required, will be treated as confidential waste and disposed of in accordance with Handling Protectively Marked Material (2007) – A Guide for Police Personnel and the Protective Marking Procedure, referred to above.

**Subject Access**

Under section 7 of the DPA 1998, individuals have a right of access to personal data held about them which they can exercise by making a subject access request. Details of the administration and processing of subject access requests can be found in the Data Protection - Subject Access Procedure.

The Records Management & Correspondence Handling Policy [link] contains more detail about the OPCC processes for subject access.

Upon request all police staff/officers/OPCC staff will supply the Civil Disclosure Unit as soon as possible with copies of any information requested to facilitate a response within the 40-day deadline.

If a directorate wishes to claim a non-disclosure exemption under the DPA 1998, to prevent information being disclosed to a subject, they should indicate what information should be withheld by highlighting the information. The FULL document/record will then be supplied to the Civil Disclosure Unit with an accompanying explanation of why the exemption should be claimed.
Further advice on this matter can be obtained from the Civil Disclosure Unit at NYP Headquarters.

**Privacy by Design**

This is an approach to project that promotes privacy and data protection compliance from the start. Although this approach is not a requirement of the DPA it will help to comply with their obligations under the legislation.

Privacy and data protection is a key consideration in the early stages of any project and then through its life cycle. Specifically when:

- building new IT systems for storing or accessing personal data
- developing legislation, policy or strategies that have privacy implications
- embarking on an information sharing initiative
- using data for new purpose.

The Project Owner should consider at the outset of any new Project whether the project could impact upon privacy and conduct an assessment as to whether a Privacy Impact Assessment would be beneficial. The Information Commissioner has issued [guidance](#) about conducting Privacy Impact Assessments and the guidance includes screening questions which Project Owners will find helpful. Privacy Impact Assessments should be completed in consultation and liaison with the Police Lawyer (Civil Disclosure).

**Police Enquiries – Access to Information Held by Other Organisations**

Occasionally information relevant to a police enquiry must be sought from other organisations. In these circumstances an organisation may request an official form from NYP, stating what specific information is sought and why. Personal data may be exempt from the provisions of the DPA 1998, in cases where the disclosure is required for the following purposes:

- prevention and detection of crime
- apprehension or prosecution of offenders

These exemptions only apply to the extent that if the data were not disclosed to the police it would be likely to prejudice investigations.

In all circumstances a Section 29(3) DPA 1998 exemption form 304 will be used. All NYP personnel should ensure that the Section 29(3) forms are completed fully and adequately deal with the issue of consent, namely, they expressly state whether consent of the data subject has been obtained, or whether it is unreasonable to do so, together with the rationale for this.

It should be noted that not withstanding s29(3) DPA 1998 it is still a matter for the organisation to determine whether or not to disclose information, as there is no element of compulsion in this respect.

A brief pocket notebook entry should also be made of these transactions. Where pocket note books are not used, then an appropriate entry must be made on the source document for each transaction.

A further area that may be readily applicable to policing, is the processing of personal information to protect the vital interests of the data subject. This is catered for within Schedules 2 and 3 of the DPA 1998. These provisions are in place where there is a genuine life or death situation (e.g. medical emergency or a potential suicide) and where the usual approach of obtaining consent is not possible
or has been unreasonably withheld. Officers should ensure that the circumstances are adequately documented and retained pending any potential challenge regarding unlawful processing of data.

**Use of Section 29(3) Data Protection Act 1998 by Other Organisations**

Other organisations may serve a notice on NYP to access information held. Normally such use will be by organisations who have the authority to investigate and/or prosecute offences. It should be noted that there is no obligation for NYP to comply with such a request and any disclosure must only be made in accordance with relevant NYP policies, procedures and/or legislation

**Disclosures required by law**

DPA section 35(1) exempts personal data from the non-disclosure provisions, where the disclosure is required by or under any enactment, by any rule of law or by the order of a court.

In this context an enactment refers to an Act of Parliament or a statutory instrument, while an order of a court refers to an order of any court or tribunal that has the status of a court. It is difficult to identify any disclosure from the police service required by any rule of law which would not also be one required either under enactment or order of a court.

Most mandatory disclosures will be Court Orders. Any Court Orders for disclosure of information must be forwarded to the Civil Disclosure Unit immediately upon receipt.

The Civil Disclosure Unit will consider whether a court order requiring disclosure of personal data is satisfactory and whether there is a necessity to exercise its ability to seek to vary the court order.

**Considering a disclosure request under section 35 DPA 1998**

When a request for the disclosure of personal data is received by NYP, and it is identified that DPA section 35(1) or DPA section 35(2) is engaged, the following should be considered by the Civil Disclosure Unit:

- the requirement under law for the disclosure
- the personal data involved
- the Schedule 2 (and where necessary Schedule 3) grounds for processing
- compliance with sixth principle
- compliance with seventh principle
- Information security and disclosure
- the need for an application for a Court Order to be varied

**Disclosures made in connection with legal proceedings**

DPA section 35(2) exempts personal data from the non-disclosure provisions, where the disclosure is necessary:
• for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings), or
• for the purpose of obtaining legal advice, or
• is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

There is no obligation to disclose personal data pursuant to a request made by a third party under DPA section 35(2). DPA section 35(2) requires that the disclosure should be necessary, as opposed to being simply desirable.

Due to the discretionary nature all requests of this nature should be referred to the Civil Disclosure Unit to ensure a uniformed approach. The Civil Disclosure Unit will have regard to the following;

• disclosures are at the discretion of the chief officer
• disclosures will not be made until the conclusion of any related criminal investigation or prosecution, and the circumstances where the CPS or coroner will be consulted
• disclosures will be based upon careful consideration of all the facts
• third-party data may form part of the requested information
• Statements provided by police officers or third parties will only usually be disclosed with the consent of the individual, unless authorised by either the Police Lawyer (Civil Disclosure) or the SIRO.
• Disclosure will only be made after careful consideration has been given to the schedules under the DPA 1998 and any data subjects rights to a private and family life under Article 8 Human Rights Act 1998.
• fees may be charged in conjunction with the fees and charges manual

Responsibilities

The chief officer (as ‘data controller’) is legally responsible for NYP’s compliance with the DPA 1998.

The Police and Crime Commissioner (as ‘data controller’) is legally responsible for NYPCC’s compliance with the DPA 1998.

The Senior Information Risk Owner (SIRO) is responsible for ensuring appropriate technical and/or organisational measures for the type of information (including personal data), together with any risks to information and the business. The SIRO:
• has ownership of risk
• ensures that information management and other risks are considered
• understands how the strategic business goals of the police force may be affected by information system failures
• is supported by the information assurance resources and others

All persons working for, or on behalf of NYP and NYPCC, having access to personal data, are required to comply with the requirements of the DPA 1998.