Data Protection Policy

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

Policy Statement

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

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

NYP and the OPFCC 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 2018 will help to deliver these benefits.

Policies and Procedures:
Appropriate Policy for the Processing of Special Category Data for Law Enforcement Purposes
Clear Desk and Clear Screen Procedure
Collection and Recording of Police Information (Niche RMS) Procedure
Data Protection – Subject Access Procedure
Data Protection – Consent Guidance
Domestic Abuse Procedure
DPIA Procedure
Freedom of Information Procedure
Information Security Policy
Internet and Email ProcedureManagement & Submission of Intelligence Information Procedure
National Crime Recording Standard Procedure
National Standards for Incident Recording Procedure
Personal Data - The right to ectification and the right to erasureProtective Marking Procedure (from September 2016 onwards)
Records Management Policy
Reuse of personal data procedure
Review, Retention and Disposal of Information Procedure
Safeguarding Children from Abuse Procedure
Security Incident Reporting Procedure

Other Documents:
APP Information Management – Data Protection

Process The Act

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. The Act includes:
- Part 2 General Data Processing Regulation (GDPR) - e.g., HR, payroll, pension data
- Part 3 Law Enforcement Directive – data collected for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data

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 means any information relating to an identified or identifiable living person who can be directly or indirectly identified by reference to an identifier such as a name, an identification number, location data, an online identifier, physical , physiological, genetic, mental, economic, cultural or social identity
- special category personal data relates to an individual's 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 living person, data concerning health or data concerning a living person's sex life or sexual orientation

The Act sets out six principles for good information, handling and processing, a full description of each can be found at the following link: ICO's guide to the six principles.

"Processing" under the act includes: *Collection, recording, organisation, structuring, stage, adaptation or alteration, retrieval, consultation ,use, disclosure by transmission, dissemination or otherwise making available, alignment or combination restriction, erasure or destruction.* This means processing is any action performed on, or using, personal data. Be direct or indirect personal data.

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.**

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

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

The principal purpose for which the OPFCC 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 OPFCC and its employees and the use of CCTV systems for crime prevention.

The Data Protection Act (DPA) 2018 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

Legal Basis for Processing Personal Data

It is important we must identify a legal basis for processing any form of personal data. Before we commence any new processing of personal data, or indeed attempt to reuse personal data for a different purpose to its original purpose, consult with the Data Protection Officer (DPO) to determine the legal basis, in turn this will ensure the recording of the legal basis, adoption of appropriate privacy notices and further advice to be provided. Privacy notices will be reviewed at least on an annual basis, however, changes to legislation or processing should trigger such reviews sooner. The DPO will prompt the Information Asset Owners (IAO) to review their privacy notices, the IAOs are responsible for notifying the DPO of changes to processes which need reflecting in the privacy notices.

The legal bases afforded to us for the processing of general information under Part 2 of the Data Protection Act 2018 – the General Data Protection Regulation (GDPR).

a) Consent – an individual gives consent to the processing of their personal data for specific purposes (please see Data Protection – Consent Guidance)*

b) Contractual – processing is necessary for the performance of a contract to which the data subject is party or in order to take steps to enter into a contract

c) Legal obligation – processing is necessary to comply with a legal obligation we have

d) Protecting vital interests – processing is necessary in order to protect the vital interests of an individual

e) Performance of a task – processing is necessary for the performance of a task carried out in the public interest **or** in the exercise of our official authority. We must be specific about which of these we're relying on and support it with a code or practice or similar if relying on the latter.

f) Legitimate interests – processing for legitimate interests pursued by us. Please note, this does not apply to public authorities in the performance of our public tasks exercised under our official authority. We may rely on this lawful basis for activities undertaken for purposes other than those performed in our official capacity.

* Where we rely on consent for processing information, business areas must ensure they have processes in place to record that explicit and informed consent has been given, to review the validity of consent (where appropriate) by way of a consent audit, and to allow the withdrawal of consent by either deleting the personal data of the individual or anonymising it to remove any personal identifiable data. Processing based on consent must be documented on the Consent Register held by the Compliance Team within Information Management.

We may also process personal data for law enforcement purposes for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. These provisions are within Part 3 of the Data Protection Act 2018 – the Law Enforcement Directive.

Information Governance Training Requirements

The minimum training requirements for all roles across the organisation in relation to information governance including training relating to data protection matters, is documented in the Training Needs Analysis which may be accessed via The Source – Business – Information Management – Documents – Training Needs Analysis for Information Governance and Data Protection requirements. The national and local training requirements are documented for roles within the workforce including: senior management roles, expert roles relating to information governance and data protection, along with roles that require more of an enhanced knowledge of data protection and courses that are mandatory completion for all roles within the workforce. The Compliance Manager and Data Protection Officer is responsible for identifying IG training based on roles across the organisation, with the support of Information Asset Owners, line managers and individuals to ensure the training is undertaken.

This is used on an annual basis to inform NYP's principal L&D requirements in line with the L&D procedure (Learning & Development (previously known as Training)), and any additional L&D requirements for expert roles as per the procedure, are considered and prioritised by the Compliance Manager and Data Protection Officer and Information Asset Owners appropriately.

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 subject access requests should be directed to the Civil Disclosure Unit.

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 2018 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 Data Protection Officer.

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
- PNC Manuals of Guidance
- Force Policy and Procedure Subsite

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 PFCC 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 PFCC. The principal purpose of notification is transparency and openness. It is a basic principle of the DPA 2018 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 Data Protection Officer and Civil Disclosure Unit has responsibilities for providing data protection advice and guidance within NYP and the OPFCC, namely:

- ensuring that guidance is available on all aspects of the DPA 2018
- 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 NPCC Data Protection Portfolio Group and the Information Commissioner

Information Security

The sixth principle of the Data Protection Act 2018 requires NYP and the OPFCC 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 Clear Desk and Clear Screen Procedure
- Internet and 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 Officer who will assess the breach and the necessity to inform the Information Commissioner's Office.

Where required, the DPO or appointed representative will notify the ICO of high risk breaches. The notification will include all requirements listed in s67 of the Act. Any additional information requested by the ICO during the course of their investigation will also be provided, save any personal data.

Where there is a need to notify the data subjects of any high risks to them, legislative requirements within Article 34 and S68 of the data protection act will be met. The preferred method of communicating high risks to the data subjects should be verbal, preferably in person by an Officer. If this is not possible, a call will be made by the DPO. Failing this, a letter will be issued.

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 Policy 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 APP's Data Protection – Handling Protectively Marked Material Procedure – A Guide for Police Personnel and the Protective Marking Procedure, referred to above.

Subject Access

Under Article 15 of the GDPR and Article 14 of the Law Enforcement Directive (S45 of the Data Protection Act), 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 Requests Procedure.

The subject access procedure contains more detail about the OPFCC processes for subject access.

Upon request all police staff/officers/OPFCC staff will supply the Civil Disclosure Unit as soon as possible with copies of any information requested to facilitate a response within one month of the request becoming valid.

If a directorate wishes to claim a non-disclosure exemption under the DPA 2018, 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 - Data Protection Impact Assessments (DPIAs)

This is an approach that promotes privacy and data protection compliance in everything we do. To be considered particularly at the beginning of a project. It is now a requirement of the Data Protection Act 2018.

You should consider data protection and privacy particularly when working with personal data in the following scenarios:

- **New technologies:** processing involving the use of new technologies, or the novel application of existing technologies (including artificial intelligence).
- **Denial of service:** Decisions about an individual's access to a product, service, opportunity or benefit which is based to any extent on automated decision-making (including profiling) or

involves the processing of special category data.

- **Large-scale profiling:** any profiling of individuals on a large scale.
- **Biometrics:** any processing of biometric data.
- **Genetic data:** any processing of genetic data, other than that processed by an individual GP or health professional for the provision of health care direct to the data subject.
- **Data matching:** combining, comparing or matching personal data obtained from multiple sources.
- **Invisible processing:** processing of personal data that has not been obtained direct from the data subject in circumstances where the controller considers that compliance with Article 14 would prove impossible or involve disproportionate effort i.e. we can not reasonably contact individuals to let them know we are processing their personal data
- **Tracking:** processing which involves tracking an individual's geolocation or behaviour, including but not limited to the online environment.
- **Targeting of children or other vulnerable individuals:** The use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children.
- **Risk of physical harm:** Where the processing is of such a nature that a personal data breach could jeopardise the [physical] health or safety of individuals.
- **Automated decision-making** with legal or similar significant effect based on personal data
- **Systematic monitoring** of using personal data.
- **Evaluation or scoring** based on personal information.
- **Sensitive data** or data of a highly personal nature.
- Data processed on a **large scale**.
- Data concerning **vulnerable data subjects**.
- **Innovative use or applying new technological** or organisational solutions.
- **Preventing data subjects from exercising a right** or using a service or contract.

Please follow this link to the DPIA Procedure for full instruction on who, when, how and why a DPIA is conducted.

As DPIAs take a systematic approach to analysing the process, data flows and risks associated with the collection of personal data, and the affects it as on privacy, it makes it best practice to incorporate the assessment at the start of any project. This allows for early intervention on any risks

identified with the proposed methods of collection and processing of data, and permits departments to address the ways in which to minimise the risks of intrusion on privacy or the misuse of personal information. It is important to mitigate any risks and where appropriate ensuring measures are in place for data minimisation and pseudonymisation. Risks will often arise by processing:

- Inaccurate, insufficient or out of date data;
- Gathering and retaining excessive or irrelevant data;
- Keeping data for longer than is necessary;
- Disclosing data to third party individuals/organisations without consent of the data subject
- Processing the personal data of an individual in ways that are unacceptable or unexpected.
- Not storing the data securely or sharing data securely

Data protection and privacy will need to be considered throughout the projects life especially if changes are required, such as new locations, new technology or additional data is to be collated. BWV cameras, facial recognition and ANPR are just a few of the more common projects where a DPIA is required.

Individuals have a right to access the information held by organisation and query the processing of their data. If data breaches occur it can be harmful to individuals who may find the processing of data both damaging and distressful and can lead to financial losses and jobs, and affect personal relationships and reputation.

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 DPA2018, 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 request for information for law enforcement purposes can be made under Schedule 2, Part 1 (2) of the Act**.** All NYP personnel should ensure that the Request for Information Form is completed fully and adequately deal with the issue of consent, namely, 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 notwithstanding the Schedule 2, Part 1 (2) element 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. 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 the Schedule 2, Part 1 (2) request for information under the Data Protection Act 2018 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 2018 Schedule 2, Part 1 (5) (1-2) 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 Schedule 2, Part 1 (5) (1-2) Data Protection Act 2018

When a request for the disclosure of personal data is received by NYP, and it is identified that DPA 2018 Schedule 2, Part 1 (5) (1-2) is engaged, the following should be considered by the Civil Disclosure Unit;

- the requirement under law for the disclosure
- the personal data involved
- the grounds for processing
- compliance with the principles
- Information security and disclosure
- the need for an application for a Court Order to be varied

Disclosures made in connection with legal proceedings

DPA 2018 Schedule 2, Part 1 (5) (3) 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 2018 Schedule 2, Part 1 (5) (3). 2018 Schedule 2, Part 1 (5) (3) 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 Data Protection Officer, Police Lawyer (Civil Disclosure) or the SIRO.
- Disclosure will only be made after careful consideration has been given to the schedules under the DPA 2018 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 2018.

The Police, Fire and Crime Commissioner (as 'data controller') is legally responsible for NYPCC's compliance with the DPA 2018.

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 2018.

Document Administration	
Head of Function (Portfolio Lead):	Sarah Wintringham, Head of Information Management
Start Date of document:	01/09/04
Author & role:	Malwina Leszczynska, Data Protection Officer
Extent of consultation: Mandatory: Legal Services Key stakeholders as required including but not limited to UNISON, Risk & Assurance Staff Associations and Heads of Departments, Health & Safety.	NYP Consultation Group IM lead Records Compliance Officer CDU
Date of Equality and Human Rights Assessment: EHRA guidance (to be assessed at draft stage and each review)	Malwina Leszczynska, 02/06/2023
Date tested against the Code of Ethics: Link to APP (to be tested at draft stage and each review)	Malwina Leszczynska, 02/06/2023
Checked against Authorised Professional Practice (APP)	Malwina Leszczynska, 02/06/2023
Date of approval by Delegated Manager:	03/12/14
Reviewer & role:	Malwina Leszczynska Data Protection Officer
Date of next review:	02/06/2026
Version :	020623
Date published onto policy/procedure/guidance subsite:	08/06/2020
Communication: Force wide e-mail / Headlines /OLB	
Publication on NYP Website (non-publication must be justifiable by the author, i.e. of operational significance)	OFFICIAL

Equality and Human Rights Assessment

Equality Section

1. What are the aims, objectives and intended outcomes of the initiative?

- Ensuring that staff undertake their legitimate duties in a manner that is compatible with the data protection principles
- Recognise the sensitivity of processed personal information and obligations in respect of data held by NYP i.e. to protect individuals from harm caused by the use of inaccurate information, or the misuse of correct information
- 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 2018 will help to deliver these benefits

2. What research has been conducted or considered and who have you consulted with and why?

No research as such required, we are unaware of race, disability etc. of requestors.
No, all checks are processed following the same ACPO guidelines provided to all forces.

3. Could there be any implications for any of the protected characteristic groups as listed below?

Please provide details for all decisions – if a negative impact has been identified please state how this impact can be justified for the initiative.				
	Positive	**Negative**	**Neutral**	**Details**
Age			**X**	All checks processed in same way
Disability			**X**	Don't know details of disability
Gender Reassignment			**X**	Don't know details of gender reassignment
Marriage and Civil Partnership			**X**	Don't know full details of marital or civil partnership status
Pregnancy and Maternity			**X**	Don't know details of pregnancy or maternity details
Race			**X**	Don't know details of race
Religion or Belief			**X**	Don't know details of religion or belief
Sex (Gender)			**X**	All checks processed in same way
Sexual Orientation			**X**	Don't know details of sexual orientation
Human Rights Section				
1. Will the initiative engage anyone's Convention Rights?				
No				
2. Will the initiative result in the restriction of a right?				
No				
3. If any of the rights are Qualified Rights, you will need to undertake a balancing exercise : a) Is the restriction on the right lawful? Is there a law which allows you to make the initiative? b) What is the legitimate aim you are trying to achieve through this initiative? c) Is the restriction necessary and proportionate? Are you restricting one person's rights to protect the rights of another individual? Is there another way to achieve the aim identified in (b)?				
Not applicable				