



Data Protection – Subject Access Procedure

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.

Right of Subject Access

The first principle of the General Data Protection Regulation (GDPR) 2018 states that personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.

Subject to exemptions, Article 15 of the GDPR and Section 45 of the Data Protection Act (DPA) 2018 provides the data subject the right to obtain from the data controller confirmation as to whether or not personal data is being processed about them, allowing individuals to verify the lawfulness of the processing.

Upon making a request both in writing, or verbal, and proving their identity, an individual is entitled to:

Under GDPR Article 15

- to be told by North Yorkshire Police (NYP) or the Office of the Police, Fire and Crime Commissioner for North Yorkshire (OPFCC) whether or not personal data concerning him or her is being processed and where that is the case, they have access to the following information
- a copy of the personal data undergoing processing
- the purposes for processing the data
- categories of personal data concerned
- to whom the personal data have been or will be disclosed
- the envisaged period for which the personal data will be stored
- the right to request from the controller rectification or erasure of personal data or restrictions of processing of personal data
- the right to lodge a complaint with a supervisory authority
- if personal data is not collected from the data subject, any available information as to their source
- be informed of the appropriate safeguards if personal data is transferred to a third country.

Under Section 45 of the Data Protection Act 2018

- the purposes of and legal basis for the processing;

- the categories of personal data concerned;
- the recipients or categories of recipients to whom the personal data has been disclosed (including recipients or categories of recipients in third countries or international organisations);
- the period for which it is envisaged that the personal data will be stored or, where that is not possible, the criteria used to determine that period;
- the existence of the data subject's rights to request from the controller
- rectification of personal data (see section 46), and
- erasure of personal data or the restriction of its processing (see section 47);
- the existence of the data subject's right to lodge a complaint with the Commissioner and the contact details of the Commissioner;
- communication of the personal data undergoing processing and of any available information as to its origin.

Subject access is a statutory right that NYP/OPFCC must accommodate. However, it should not be seen as an alternative or replacement for routine disclosures or good business practice. Staff should, where possible, engage with individuals to ensure that their problems are resolved rather than forcing them into subject access applications.

While personal data often forms part of a document, it is important to recognise that the right is one of access to personal data and not necessarily the full document. For access to other types of information, please see the Freedom of Information Procedure.

Overarching Policies:

Records Management Policy

Procedures:

Data Protection Procedure

Deletion of Records from National Police Systems Procedure

PNC Procedure

Freedom of Information Procedure

Other Documents:

ACPO Data Protection Manual of Guidance

Data Protection Act 2018

Criminal Procedures and Investigations Act (CPIA) 1996

Rehabilitation of Offenders Act 1974

The Limitations Act 1970

Process

Availability of Application Forms

A subject access request can be made either completing the online form on the North Yorkshire Police website, printing and completing the Subject Access PDF form provided on the website, by written correspondence, or by a verbal request to an Officers/Staff member. Forms shall not be provided to businesses for the purpose of conducting vetting enquiries (also see Prohibition of Requirement to Produce Relevant Records previously known as Enforced Subject Access).

Application forms are available from:

- All police stations
- NYP website ([I'd like to request information about myself | North Yorkshire Police](#))
- OPFCC website ([Subject access requests - York & North Yorkshire Office for Policing, Fire, Crime and Commissioning \(northyorkshire-pfcc.gov.uk\)](#))
- By post

Dealing with Subject Access Applications

There are various ways applications can be received into NYP/OPFCC:

- applications received at Headquarters will be dealt with by the Civil Disclosure Unit
- applications can be received at any NYP station
- applications received by the PFCC are handled in accordance with the Records Management & Correspondence Handling Procedure of the PFCC

The receiving officer will check the following:

- the application form is correctly completed and legible
- two forms of official identification are enclosed

Where the application is unsatisfactory, this should be communicated to the applicant in a timely manner, outlining all issues identified with the application.

Proof of Identity

It is important to confirm the identity of the person making the application to ensure that personal data is disclosed to the data subject and not someone impersonating them.

As a minimum, applicants are required to provide at least two different official documents, which between them, provide sufficient information to prove the applicant's identity:

- Name
- Date of birth
- Current address

For example, a combination of driving licence, medical card, birth/adoption certificate and any other official documents which show name, date of birth, address.

Examples for current address include utility bill (gas, water, electric or telephone) council tax bill, bank / credit card statement, correspondence from the Inland Revenue or Benefit Agency, mortgage lender, professional body, solicitor's letter, correspondence from your employer (payslip / letter of appointment).

Photocopies will be accepted. If the applicant is not able to provide identification, staff must contact the Civil Disclosure Unit for further information.

NYP/PFCC staff may require and request further information to satisfy themselves as to the identity of the applicant and will inform the applicant of that requirement where necessary.

Where applicants have indicated their intention to send identification through the post, they should be informed either verbally or in writing, that NYP/the PFCC will not be held accountable for any identification documents lost in the post. Identification documents will be returned to the applicant by recorded delivery.

Applicants not wishing to post their identification documents may bring the relevant documents, together with their application and prescribed fee to any NYP station for processing.

A record of any and all reference numbers for documents shall be recorded and entered on the subject access application form.

Verbal requests

If a verbal request has been made to an Officer and the Officer is satisfied as to the identity of the data subject, no further ID will be required. However, where identification cannot be confirmed then a request shall be made for further verification. A request only becomes valid once identification is verified and satisfactory information to allow us to process the request has been provided .

Receiving Officer Actions

Upon receiving a completed application form, staff shall endorse the “Police Use Only” section of the application form to record:

- that they have checked the form and all sections are completed and legible
- the types of identification supplied, together with all relevant reference numbers (e.g. driving licence number, passport number, etc.)
- the date the application was received

The application shall not be accepted by staff where:

- it has not been fully completed
- it is illegible
- identification is neither supplied, nor identifies the individual’s name, date of birth, current address and signature.

Due to the limited response period, application forms shall be sent immediately by email to the Civil Disclosure Unit, Legal and Compliance Services Directorate at NYP Headquarters.

Applications sent or received directly by the Civil Disclosure Unit shall be scanned (including the ID) and logged on to their Case Management System and processed by the department.

Where the data subject requests information relating to prosecution, convictions and cautions these applications will be forwarded to:

ACRO Criminal Records Office
ACRO (SAO)
PO Box 623
Fareham
Hampshire
PO14 9HR

Subject Access (acro.police.uk)

+44 (0)2380 479 920

customer.services@acro.pnn.police.uk

ACRO will respond directly to the data subject in relation to all requests for this category of information.

Changes of Address

If the applicant changes address during the response period, they must inform the Civil Disclosure Unit of the change of address in writing. If a change of address is notified after an application has been submitted, the applicant will be required to provide further proof of identification.

It is acceptable that persons other than the applicant may submit subject access forms. However the officer receiving the application form must be certain that it is a genuine application and not an attempt to obtain information about another individual.

Response Period

A full response will be made within one calendar month from the date the completed application/verbal request and ID was received by NYP/the PFCC.

If the request is seen to be complex or numerous, the authority is able to extend the period of compliance by an additional 2 months.

All responses will normally be sent directly to the applicant at their home address. However, there may be occasions when the applicant specifically requests that information should be sent to their solicitor or by email. Such requests must be stated at the time of the request and any authorisation forms signed by the relevant persons e.g. solicitor. Arrangements can also be made so that the applicant attends NYP/PFCC premises to collect the response in person. In the latter scenario, the person's identity will need to be confirmed when the information is disclosed. In the unlikely event that the one calendar month statutory period will not be met, the applicant should be contacted to advise them of the delay.

Insufficient Information

If an applicant does not provide sufficient information as may be reasonably required by NYP/the PFCC to locate the requested personal data, the Civil Disclosure Unit will inform the applicant that further information is required. This should be expedited as soon as possible after receiving an application. The one calendar month period will commence from the date the required information has been received.

Where additional information is required for the location of information, the applicant will be contacted and clarification will be sought. It may be useful for the applicant to answer questions such as:

- why do they believe their personal data is being processed?
- what contact have they had with NYP/the PFCC?
- under what circumstances did they have contact with NYP/the PFCC?
- when and where any contact has been made?
- to provide any other details which either NYP/the PFCC or the applicant may feel is necessary to locate any information held

In most circumstances, a subject access application ‘for everything you hold about me’ would in itself constitute insufficient information. However, there may be limited occasions where the nature of the relationship between the applicant and NYP or the PFCC, and the context of the request, makes such a request sufficient.

Where the application is for unstructured personal data, the application must include a description of the data.

Applications Made on behalf of Another (Agents/Power of Attorney/Persons with Disabilities)

In such circumstances, NYP/the PFCC may be provided with suitable written evidence to confirm that the person has the power to act on behalf of the data subject.

Applications Made on behalf of Another (Young Person)

Subject access applications can be accepted from a young person where they are believed to have sufficient intellectual ability to understand the nature of the application.

It is generally presumed that a person of thirteen years of age or more will have sufficient age and maturity to exercise the right of subject access. In other cases, a child under that age will still be able to exercise the right where they have a sufficient general understanding of what it involves. A parent or guardian can exercise the right and receive the reply, if the young person does not have the necessary intellectual ability to understand the nature of the application, and the parent is thought to be acting in the best interests of the young person. Cases that are borderline will be reviewed against the following:

- The child’s level of maturity and their ability to make decisions like this;
- The nature of the personal data;
- Any court orders relating to the parental access or responsibility that may apply;
- Any duty of confidence owed to the child or young person;
- Any consequences of allowing those with parental responsibility access to the child’s or young person’s information. This is particularly important if there have been allegations of abuse or ill treatment;
- Any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- Any view the child or young person has on whether their parents should have access to information about them.

Consideration must be given to requesting the young person’s birth or adoption certificate or other evidence to show the parent or guardian has parental responsibility for him/her.

Caution must be exercised when dealing with such applications where it is clear that the young person’s parents are in dispute with one another and/or the application may not be in the best interests of the young person.

Manifestly unfounded or Excessive requests

GDPR Article 12(5) and DPA 2018 Article 53 states that where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the authority may charge a reasonable fee based on administrative costs or refuse to action on the request. If this is the case then NYP or the PFCC will notify the data subject of the reasonable fee, or the refusal of their request and provide information in relation to their rights to complain to the supervisory authority and to a judicial remedy.

North Yorkshire Police Upper Limits for Excessive Effort

There may be occasions where data retrieved to satisfy the terms of the applicant's request are so vast that to view every item would be excessive as well as the requirement of staff resources to review such requests. To assist the review in such cases an upper limit has been assessed for the following listed assets.

Emails – Limit to 360 messages

This limit assumes that a search has been conducted on E-disclosure and the search criteria has already been refined, with the applicant, to a point that applying a further filter would risk removing the applicant's personal data.

It is measured in that preparing **5 email messages** from their initial state to PDF and then to being fully redacted would take **15 minutes**.

Multiplied out, the 18 hour threshold in the Freedom of Information Act 2000 is crossed at **360 messages**. The Freedom of Information Act 2000 threshold is referred to for guidance and best practice in estimating processing times for retrieving and determining if information is held.

If a refinement is not offered by the applicant, then the excessive effort will be considered, and the request refused.

Body Worn Video (BWV)

If a request for Body Worn Video / CCTV footage is received, the request will be highlighted by the logger with the line manager and a search will be conducted to ensure that any relevant footage is saved.

Before BWV footage is provided, clarification will be sought from the applicant and the following options will be considered:

If a large amount of pixilation of third parties is required, then to assist the applicant a set of screenshots will be provided, roughly ten minutes apart (where they are visible). This will also help to establish which parts of the footage they actually require.

If there is more than one BWV, but all cameras show the same event, then only one BWV (the one showing the most footage) will be provided, as this will be deemed as reasonable.

If the full scope of the footage is still requested then the amount of time that it will take to redact/edit the footage will be considered and if there is over 18 hours of work required then a **reasonable** charge will be applied for the preparation of the information.

Withholding Information and Personal Data

A combination of provisions covering third-party personal data, disproportionate effort and exemptions, may restrict access to personal data sought under the subject access process. In addition, there may be instances where other statutory obligations further restrict the disclosure of personal data. See the restrictions section.

Third Party Personal Data

NYP/the PFCC may not be obliged to disclose/ comply with a request if disclosing the information would identify another individual. If the source of the personal data identifies a third-party then it can be withheld, a process which is usually achieved by editing or redacting the response.

Information about a third party can only be disclosed if:

- the third-party has given consent to the person making the request
- it is reasonable in all the circumstances to reply to the request without the consent of the other individual

In these circumstances, due regard has to be given to balancing the interests of the parties concerned. In deciding this question, regard should be had to any duty of confidentiality owed to the other individual, any steps taken by NYP/the PFCC with a view to seeking the consent of the other individual, whether the other individual is capable of giving consent and any express refusal of consent by the other individual.

Specific measures may need to be taken when responding to applications for access to CCTV material. It may be necessary to blur any images of third parties on the material unless they do not have a reasonable expectation of privacy, for example, if they are in a public place.

Subject Access Restrictions

There are a number of restrictions within the Data Protection legislation that recognise that there may be a public interest in withholding personal data sought under subject access. These exemption will be applied where necessary to any information held in respect of the data subject.

Restrictions must not be used as a 'blanket' to withhold everything the police hold on an applicant. They will be used on a case-by-case basis and only to the extent required.

Information may be withheld if it is necessary and proportionate to safeguard:

- National Security
- Defence
- Public security
- The prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties including the safeguarding against and the prevention of threat to public security
- Other important objectives of general public interest of the Union or of a Member State, in particular an important economical or financial interest of the Union or of a Member state, including monetary, budgetary and taxation matters, public health and social security
- The protection of judicial independence and judicial proceedings

- The prevention, investigation, detection and prosecution of breaches of ethics for regulated professions
- A monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority
- The protection of the data subject or the rights and freedoms of others
- The enforcement of civil law claims

Restrictions under GDPR

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679>

Restrictions under DPA 2018

<http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted/data.htm>

Regulatory functions relating to legal services, the health service and children's services.

Where an exemption is applicable to an application, a response will be sent to the applicant and informed of their rights to complain to the supervisory authority and to a judicial remedy.

In cases where the personal data had already been officially released to the applicant through disclosure under the Criminal Procedures and Investigations Act (CPIA) 1996 it is unlikely that the exemption would apply.

Data Portability

Article 20 – GDPR states:

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:
 1. the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and
 2. the processing is carried out by automated means.
2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.
3. ¹The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. ²That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

Art. 20 GDPR – Right to data portability - General Data Protection Regulation (GDPR) (gdpr-info.eu)

Data will therefore be provided in a PDF version or paper version. If Discs are used for releasing footage, then this will be done in an encrypted format and files will be sent in an MP4 format, where possible. VLC is a free software that can be downloaded by data subjects, which is required to view the footage. Guidance on how to extract the data file will be provided if required.

Digital information can also be provided through Egress business accounts, which is a secure portal. The portal is only sent to the data subject and allows them to access the portal to download disclosures that have been sent / relate to them. This is an option that has been created for larger files, which cannot go via normal email.

Information other than Personal Data or Third Party Personal Data

In most cases when personal data is retrieved for disclosure to a subject access applicant, that personal data will be surrounded by other information which will not be the applicant's or another's personal data. For pragmatic reasons this 'other information' may be disclosed to the applicant. NYP and the PFCC must recognise that this represents a provision of information beyond that required by the Data Protection legislation. Release of this type of information is on a purely discretionary basis only and there is no obligation to release it.

Routine Amendment and Deliberate Destruction

The information supplied in response to a subject access application must reflect the personal data held at the time the application was accepted by NYP or the PFCC. However, account may be taken of any routine amendment or deletion made between receiving and responding to an application, provided that it had not been made as a result of receiving the application.

It is an offence under Part 6, Section 173 of the Data Protection Act 2018, to alter, deface, block, erase, destruct or conceal information with the intention of preventing disclosure.

Personal Data Derived from another Body

NYP and/or the PFCC is obliged to consider all personal data in their possession when they receive a subject access application, irrespective of where that personal data originated from. Some applications are likely to encompass information which was provided by or created by third party organisations or individuals (i.e. not NYP/the PFCC or the applicant). Examples would include personal data contained in documents created by other police forces, doctors, solicitors, CPS etc.

In such cases, and where practical, NYP/the PFCC may choose to write to the provider of the information to explain that an application has been received and ask formally for their views on disclosure of any personal data to the applicant, on the basis that the provider would be in a position to comment on exemptions relevant, from their perspective. The correspondence could indicate that unless an objection was received before the end of the one calendar month deadline, NYP/the PFCC may consider the disclosure of the personal data sought.

In all cases, irrespective of the provider's comments, the final decision on disclosure rests with NYP/the PFCC.

Prohibition of Requirement to Produce Relevant Records (previously Enforced Subject Access)

DPA 2018, Part 7 section 184 states that it is an offence for a person to require another person to provide information in connection with recruitment, continued employment or for the provision of goods or services. They should instead be using the existing formal criminal records check

arrangements operated by the Disclosure and Barring Service, Disclosure Scotland or Access Northern Ireland.

This may be interpreted as contrary to the spirit of the Rehabilitation of Offenders Act 1974, as in some cases it forces those individuals to reveal 'spent' offences that they would not have to disclose if the provisions of the ROA 1974 were applied.

Criminal Procedure and Investigations Act 1996 (CPIA)

Where a subject access application results in the disclosure of copies of intelligence, crime files, or prosecution files, a record of, or reference to, that disclosure will be made and where possible incorporated in the original documentation. This may assist in alerting staff to the fact that a disclosure had been made and thus assist compliance with the requirements of the CPIA 1996.

Appeals and Complaints Process

Should an applicant feel that they have cause to complain, either in relation to the information held on NYP/PFCC systems, or in relation to the way in which their subject access application has been handled, they have a right to make a formal complaint.

Complaints relating to any inaccuracies, erasure or restriction of processing should be made in writing to the Review, Retention and Disposal Unit RRD@northyorkshire.police.uk who will review the request in accordance with the legislation.

If a complainant wishes to complain about the way in which their information is being processed they have the right to complain directly to Data Protection Officer about the processing of their personal data dataprotectionofficer@northyorkshire.police.uk

The Data Protection Officer may contact the complainant for further information or clarification in order to resolve the complaint.

Individuals can also complain to the Information Commissioner. Further information can be obtained from the <https://ico.org.uk/>

If the complainant wishes to complain about a member of staff, then they need to make their complaint to:

Force Solicitor and Head of Legal Services
North Yorkshire Police Headquarters
Alverton Court
Northallerton
North Yorkshire
DL6 1BF

Where a complainant states that they wish their information to be removed from PNC due to exceptional circumstances, they will be directed to the PNC Retention Policy Exceptional Case Procedure.

Further information can be found on the website: [Information Rights | North Yorkshire Police](#)

Monitoring of Subject Access Requests

The following areas of the Subject Access process are to be monitored on a regular basis by the Data Protection Officer:

1. Application of exemptions
2. Redaction

A dip sample of subject access requests will be reviewed periodically to monitor the above areas. The monitoring will then be recorded on the subject access request database.

Review and Retention of Subject Access Application Information by Police Forces

In accordance with the Data Protection Act principles, NYP shall adopt a standard retention period of two years for summary details of 'National' subject access applications (i.e. those sent to the ACRO). At the conclusion of the two-year period the continued retention of that information will be reviewed, and where it is no longer justified the information will be destroyed.

NYP and the PFCC will also adopt a standard retention period of two years for all information related to 'local' subject access applications. At the conclusion of the two-year period the continued retention will be reviewed, and where it is no longer justified the information will be destroyed.

NYP and the PFCC will attempt to distinguish between 'routine' subject access applications and others where the circumstances may suggest longer retention would be prudent. Factors to consider include:

- whether the NYP or PFCC's handling of the application has been, or is likely to be, subject to complaint
- whether it is high profile in nature
- whether the application involved the use of 'unusual' exemptions
- where there is a possibility that legal action could ensue

Other legislation may be of assistance in identifying if information is required to be kept for longer than two years. Cognisance should be particularly paid to periods defined in The Limitation Act 1980.

Document Administration	
Head of Function (Portfolio Lead):	Xanthe Tait – Director of Tri-Legal Services
Start Date of document:	01/01/07
Author & role:	Simon Dennis, Director of Legal & Compliance Services Directorate
Extent of consultation: Mandatory: Legal Services & Information Management. Key stakeholders as required including but not limited to UNISON, Risk & Assurance Staff Associations and Heads of Departments, Health & Safety.	This is a statutory requirement no further consultation is required
Date of Equality and Human Rights Assessment: EHRA guidance (to be assessed at draft stage and each review)	Caroline Williams, Team Leader (Civil Disclosure) 18/01/2022

Date tested against the Code of Ethics: (to be tested at draft stage and each review)	Caroline Williams, Team Leader (Civil Disclosure) 18/01/2022			
Checked against Authorised Professional Practice (APP)	N/A			
Date of approval by Portfolio Lead:	20/06/2024			
Reviewer, role, and date completed:	Naomi Mackenzie, Data Protection Senior Support Officer, Information Management Department, Legal Services 07/01/2022			
Date of next review:	07/01/2025			
Version:	200624			
Date published onto policy/procedure/guidance subsite:	27/06/2024			
Communication: Force wide e-mail / Organisational News				
Publication on NYP Website (non-publication must be justifiable by the author, i.e. of operational significance)	OFFICIAL			
Equality and Human Rights Assessment				
<u>Equality Section</u>				
1. What are the aims, objectives and intended outcomes of the initiative?				
Subject to exemptions, NYP will provide individuals with a right of access to personal data of which they are the subject. This process is known as the right of subject access. Upon making a request in writing, and proving their identity, an individual is entitled (subject to exemptions): • to be told by NYP whether it or someone else on their behalf is processing that individual's personal data • to be told, in an intelligible manner of all the information, which forms any such personal data. Subject access is a statutory right that NYP must accommodate.				
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.				
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.				
No, all checks are processed following the same ACPO guidelines provided to all forces.				
	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 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

<u>Human Rights Section</u>
<u>1.</u> Will the initiative engage anyone's Convention Rights?
No
<u>2.</u> Will the initiative result in the restriction of a right?
No
<u>3.</u> 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)?
xxx