DP 001 – DATA PROTECTION PROCEDURE – DATA SUBJECT ACCESS RIGHTS – ACCESS TO INFORMATION

Version	2.0	Last updated	10/10/2018	Review date	25/11/2018
Equality Impact Assessment			Not completed		
Owning department			Information Management Unit (IMU)		

Data Protection: Data Subject Rights – Access to Information

Nottinghamshire Police recognises that any personal data it processes must be managed in accordance with the Data Protection Act 2018.

1. About This Procedure

1.1. Section 45 of the Data Protection Act 2018 gives any individual the right of access to their own personal information held by a Data Controller.

1.2. This document seeks to replace the current procedure in place for dealing with requests for personal information which are known as 'Subject Access Requests' under the Data Protection Act 1998.

1.3. This procedure applies to all requests for personal information from Data Subjects received on or after 25 May 2018. Any requests received prior to this date will be dealt with under Section 7 of the Data Protection Act 1998.

1.4. RIGHTS OF THE DATA SUBJECT

An individual has a right to access their personal information held by a Data Controller under the Data Protection Act 2018. Under this Act individuals have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and the following supplementary information;
- the purposes for which the data is being processed
- the categories of personal data concerned;
- the recipients or categories of recipient the personal data has been disclosed to
- the retention period for storing the personal data or, where this is not possible, your criteria for determining how long it will be stored
- the existence of the data subject's right to request rectification, erasure or restriction or to object to such processing;
- the right of the data subject to lodge a complaint with the ICO or another supervisory authority;
- information about the source of the data, where it was not obtained directly from the individual;
- the existence of automated decision-making (including profiling); and
- the safeguards provided if the personal data has been transferred to a third country or international organisation.

1.5 RIGHTS OF THE DATA CONTROLLER

The Chief Constable (as Data Controller) may refuse or restrict access to information where disclosure may have a prejudicial effect on the following Policing purposes;

a) the prevention and detection, or
b) the apprehension or prosecution of offenders

Or where it would have a detrimental effect on public or national security or the rights and freedoms of others.

The Chief Constable has the right to ask that the Data Subject to provide documentation to verify their identity.

If the request is deemed 'manifestly excessive or unfounded', The Chief Constable has the right to:

- charge a reasonable fee taking into account the administrative costs of providing the information; or
- refuse to respond

Where a request is refused on the grounds of being manifestly excessive or unfounded the Data Subject will be advised of this.

2. Procedure

2.1. RECEIVING A SUBJECT ACCESS REQUEST

Any request from a member of the public which appears to be asking for information/records held by Nottinghamshire Police should be forwarded to the Information Management Dept either via the Data Protection email inbox (if received via email/Social Media), through the internal mail (if received in the post) or to Ext 318 0888 (if received via telephone). If forwarding a hard copy paper request then the letter should be date stamped with the date the correspondence was received in Force prior to transfer. This will allow the Information Management Dept to accurately calculate the deadline for response to such requests which is 1 month (28 calendar days) from the date of receipt.

If a request is received by an individual in person either at a Custody Suite or at a Police Station Front Counter staff should complete a DPA 2018 Subject Access Request form with the individual or ask the individual to complete the form themselves if they are willing to do so (copies will be available via Force Forms or through our website) and take a copy of their identification document as detailed in Section 2.1. These should then be date stamped and forwarded to the Information Management Department via internal mail as soon as possible.

The Information Management Dept will acknowledge the request and advise the applicant further.

All requests will be acknowledged by the Information Management Dept in writing and submitted via the same means as communication is initiated by the data subject where possible.

Although an individual does not have to make a written request under DPA 2018, Nottinghamshire Police are not obliged to supply any information to an individual until we:

a. Have enough information to complete the request
b. Have confirmed the individual's identity (see Identification for further information)

If receiving a telephone call from a member of the public asking for information held about

themselves by Nottinghamshire Police, staff may wish to direct them to the Subject Access form on our website which the Data Subject can complete and return to the Information Management Dept either via email or in hard copy through the post. It is important to note that a Data Subject is not obliged to complete this form in order to make a valid request under this right; however, the form will assist the applicant in providing enough detail and supporting identification documents to ensure that their request becomes valid under the recital.

As per Section 2.1 all requests made to Nottinghamshire Police for disclosure of information under the Data Protection Act 2018 will require identification verification before disclosure can be facilitated.

2.1 VERIFICATION OF IDENTITY

The controller shall use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests.

All requests for information received by Nottinghamshire Police will require the applicant to provide proof of identity. Minimum requirements to satisfy identity verification should be a document/record which verifies the Data Subject's **name, address and date of birth.** For any requests relating to obtaining video or photographic records such as Custody photographs or Body Worn Video footage, photographic identification must be produced.

The identity of the data subject must be validated on all occasions before disclosure of information is made to them.

This proof of identity may include:

Birth/adoption certificate
Marriage certificate
Driving licence
Medical card
Passport
Pension book/statement
Benefits statement
Insurance certificate (not schedule)
Hire purchase agreement
Or, any other official certified document.
Utility bill
Telephone/Mobile statement
Bank statement
Credit/debit card statement
Council tax bill
Rent book

Requests identifying photographs or videos will require **photographic** proof of identity–

Passport
Photo driving licence

Identity cards
Bus passes/membership cards, etc (*an additional proof of identity will also be required*)

Copies of identification will be scanned to the request record held on 'Cyclops' by the Information Management Department and kept for a maximum of 24 months from the date the request is closed in line with our retention schedule.

2.2 CONSENT FOR RELEASE OF INFORMATION TO THIRD PARTIES

An individual can ask for information disclosure to be made to a third party acting on their behalf such as a Solicitor.

Consent of the data subject is defined as:

Any freely given, specific informed and unambiguous indication of the data subject's wishes by which he or she by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

In order to facilitate disclosure to a third party, the Data subject will need to provide explicit and specific consent at the time of making their request. This can take the form of:

I. A short statement within the request affirming that disclosure is to be made to a third party and details of that party along with the specific description of the information to which the consent relates
II. Completing a Nottinghamshire Police explicit consent form and disclosing it along with their request (a copy of this consent form can be obtained from the Information Management Dept and is also available on our website).
III. By completing Section 2 of the DPA 2018 Subject Access Request Form available on our website.

Identification of the Data Subject will still need to be provided.

2.3 REQUEST DETAILS AND SOURCING INFORMATION

The Data Subject should identify the information to which he or she requires access by providing a description of this information within their request. This can include incident or occurrence numbers or dates and times when the information is likely to have been captured.

Recital 63 states:

Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates.

Therefore, any requests which do not appropriately identity the information being asked for may be subject to further correspondence from the Information Management Dept asking for clarity as to the specific information being sought. Where this occurs, the request will not be actioned until the Information Management Dept is in receipt of the further clarification being sought. The 28 day 'clock' will be suspended until the further information is received.

Once Nottinghamshire Police is in receipt of a validated Subject Access request it will be

recorded on our request management system; 'Cyclops' and assigned to a Disclosure Officer to research the requested information and consider disclosure under the legislation. All validated requests will be acknowledged by the Information Management Dept in writing. All details provided within the Subject Access Request will be held for the purposes of facilitating disclosure in line with the Data Subjects rights of access. Copies of requests and accompanying documents will be scanned to the request record held on 'Cyclops' retained for a maximum of 24 months from the date the request is closed. This is in line with our retention schedule.

The Disclosure Officer will review the information being requested and access the appropriate computer systems in order to locate the records/information being sought. These records will then be saved to the Information Management Department's request management system; 'Cyclops' for disclosure to be considered and facilitated. The Disclosure Officer will apply any redactions and restrictions on access to information as legislated by the Data Protection Act and record the decisions for these on Cyclops. This includes the redaction of third party and operationally sensitive material.

During the course of their research, the Disclosure Officer may have cause to liaise with individual Police Officers or Departments in order to locate any specified records or information falling within the scope of the Data Subject's request. The Disclosure Officer must not be impeded in this research and any records requested by the Disclosure Officer should be provided to them in order for them to consider any exemptions on disclosure.

The Disclosure Officer may seek the view of individual Police Officers and Departments on specific disclosure; however, it is the responsibility of the Disclosure Officer to apply any appropriate exemptions on disclosure. Any exemptions placed on disclosure should be done in line with the Data Protection legislation.

2.4 DISCLOSURE

Under the DPA 2018, an individual is only entitled to their own personal information held by a data controller. The Disclosure Officer will review records located as a result of their research and will remove any information which relates to a third party, any information which is tactically sensitive or any information which falls within an exemption under the legislation. This redaction will be applied using the electronic redaction software incorporated within the 'Cyclops' programme. Redactions will be represented by a black panel over the removed information. Redactions will be burned into the document to ensure that any electronically disclosed material will not be able to be un-redacted by the recipient.

The Data Subject will be advised as to why material has been removed via application of a 'redaction stamp' within the disclosure.

Disclosure will be made either in hard copy or via electronic means such as email dependant on the wishes of the Data Subject. If no preference is specified by the Data Subject at the time of making their request, response will be made via the same method as the request is made where possible e.g. emailed requests will be responded to via email.

Emailed disclosure will be composited into a PDF document which may be password protected (if required) and sent to the Data Subject to the email address specified within their request. The determination as to whether the document should be password protected

will depend on the sensitivity and GCS marking of the records being disclosed. Where disclosures have been password protected, the Data Subject will be required to contact the Information Management Department to access the correct password. This is to protect the Data Subject against unauthorised access to any sensitive or confidential information being disclosed.

Hard copy disclosures will be sent to the applicant via special delivery to ensure safe receipt of the requested information. Such delivery method will require the applicant to be available to sign for the delivery.

Data Subjects can choose to collect their disclosure from their nearest Police Station. This preference must be specified to the Information Management Department prior to the disclosure being made and is only available from Police Stations which operate a staffed Front Counter service. The Disclosure Officer will arrange this with the specified Police Station and Data Subject. The Data Subject will need to show valid original identification prior to collecting the disclosure and may be required to sign a receipt to indicate that the disclosure has been collected. Disclosures cannot be collected from the Force Headquarters.

A copy of the completed response will be held on the request record held and kept for a maximum of 24 months from the date the request is closed in line with our retention schedule.

2.5 TIMESCALES

Requested information should be provided without delay and at the latest, within one month of receipt of the request. For the purposes of the Act, one month is defined as **28 calendar days**.

The 28 day 'clock' will not start until the Information Management Department is in receipt of all the required information to enable it to progress the request such as identification documents and clarification as to the specific information being requested.

Where further information or identification documents are required, the Information Management department will notify the applicant in writing. The request will not be actioned until the Information Management Dept is in receipt of the further clarification/information required. The 28 day 'clock' will be suspended until the further information is received.

If the further information or clarification is not received within 28 days of being requested by the Information Management Department, the request will be closed and the applicant informed in writing. The request can be reopened at any time upon receipt of the requested information from the Data Subject.

Where a request is overly complex or involves a large number of records to be reviewed, the deadline for compliance can be extended by the Information Management Team by an **additional 2 months (56 calendar days).** Where this applies, the Data Subject will be notified in writing within the initial 28 calendar day deadline.

2.6 MANIFESTLY UNREASONABLE, EXCESSIVE OR UNFOUNDED REQUESTS

If the request is deemed 'manifestly unreasonable, excessive or unfounded', The Chief Constable has the right to:

- charge a reasonable fee taking into account the administrative costs of providing the information; or
- refuse to respond

Data Subjects could potentially attempt to use the Subject Access process as a means to harass Police Forces with no real purpose than to cause disruption. An example of this can be repeated requests for the same information over a short period of time (or over several years) or where the Police Force has provided the Data Subject with their personal data through an alternative disclosure mechanism e.g. pre-trial information being disclosed under CPIA and the same information being requested through a Subject Access Request.

'Excessive requests' can refer to those which would involve a disproportionate effort to respond to.

'Unfounded requests' are those which are clearly without basis or where the request is not made out.

Any request which asks for "all information held about me" or "all emails in which my name is mentioned" will both be considered to be manifestly excessive and/or unfounded and will be rejected for further refinement from the data subject.

In the event that a request is refused by Nottinghamshire Police the Data Subject will be informed in writing within 28 days of receipt of the request. The Data Subject will be advised as to the reasons their request is being refused and given details on their right of appeal to the Information Commissioner.

Disclosures provided in response to initial subject access requests to Nottinghamshire Police and which are facilitated via email or by the data subject collecting in person will be provided free of charge unless they are deemed to be excessive. Subsequent requests made by the same applicant for the same information within a 60 day period will attract an administrative fee which must be paid prior to any information being disclosed.

2.7 FEES

The majority of Subject Access Requests will not involve a fee. Information will be provided free of charge to any individual making a Subject Access Request unless:

- The request is manifestly unreasonable, excessive or unfounded
- The request asks for a further copy of information which has already been disclosed

Any fees deemed relevant by Nottinghamshire Police will be based on the administrative cost of providing the information only.

In the event that Nottinghamshire Police deem a fee to be chargeable in response to a Subject Access request, the Data Subject will be advised in writing by the Information Management Team within 28 days of receipt of the request. The disclosure will not be facilitated until such time as the required fee is received by Nottinghamshire Police.

Disclosures provided in response to initial subject access requests to Nottinghamshire Police and which are facilitated via email or by the data subject collecting in person will be provided free of charge unless they are deemed to be excessive. Subsequent requests made by the same applicant for the same information within a 60 day period will attract an administrative fee.

Hard copy disclosures will be sent to the applicant via special delivery to ensure safe receipt of the requested information. Such delivery method will require the applicant to be available to sign for the delivery.

2.8 REQUESTS FOR CONVICTION INFORMATION HELD ON THE POLICE NATIONAL COMPUTER

Requests for copies of conviction records or copies of any information held on the Police National Computer (PNC) will be facilitated by ACRO Criminal Records Office and NOT Nottinghamshire Police.

Such requests should be made directly to the ACRO Criminal Records Office as per the details on their website:

https://www.acro.police.uk/subject_access.aspx

Any request for PNC records received by Nottinghamshire Police will be rejected and the applicant advised to redirect their request to the ACRO Criminal Records Office.

2.9 OTHER MEANS OF DISCLOSURE

It is important to note that whilst superseding the existing rights of access to personal information as stipulated within Section 7 of the Data Protection Act 1998, DPA 2018 Right of Access legislation does not supersede all existing methods of disclosure.

There are existing means of information request/disclosure which will continue to operate as normal such as:

- DBS disclosure for employment will still be facilitated through the Disclosure and Barring Service
- Requests for copies of Custody Records and interview recordings under PACE must still be facilitated as usual practice
- Victim updates in relation to on-going criminal investigations should still be facilitated in line with the Victims Code of Practice.

2.10 CALLS TO CONTROL ROOM ASKING FOR INCIDENT/OCCURRENCE NUMBERS

When a member of the public calls up for basic information such as an incident or crime number, **providing you are satisfied that they are the person entitled to the information** (possibly by asking them to verify basic details as recorded on the incident such as their name and date of birth, or the location of incident), it is OK to pass the incident number or Niche Occurrence number only.

2.11 ENFORCED SUBJECT ACCESS REQUESTS

Certain employers and organisations such as recruitment agencies may attempt to exploit the subject access process by requiring individuals to use it to obtain a copy of their criminal convictions (or evidence that there is nothing held) as part of recruitment or continuing employment processes.

This practice is known as enforced subject access as covered by Section 184 of the Data Protection Act 2018. It is a criminal offence for a current or prospective employer or recruitment agency to require an individual to make a subject access request as a condition of 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.

Where a subject access request is made and the applicant clearly states that the information is for employment purposes, the request will be rejected and the data subject will be redirected to the appropriate agency.

The applicant can identify whether they have been asked to seek disclosure from an agency within Part 5 of the Subject Access request form. Positive indication will not affect the data subject's right to information under the Act and their request will continue to be processed as per the Act, however, the Information Commissioner should be notified of the request.

2.12 **SUBJECT ACCESS REQUESTS FROM CHILDREN**

Children are to be afforded the same rights regarding access to their information as is given to adults as long as they are competent to do so. Under Scottish legislation, a child has been considered to be able to apply their subject access rights at age 13. Where a child is not considered to be 'competent', an adult with parental responsibility may exercise the child's data protection rights on their behalf.

The parent must provide proof of parental responsibility in these cases as well as valid identification for themselves. Disclosure will not be facilitated until we are in receipt of such documents as required to validate the requestor's identity and parental responsibilities to the child in question.

3. Monitoring and Evaluation

3.1. The adherence to, and the effectiveness of this procedure, will be monitored by the Information Management Unit.

4. Review

4.1. This procedure will be reviewed after 6 months and then yearly
4.2. The review will take account of changes in legislation and working practices, as well as consultation with relevant internal and external stakeholders.
4.3. Information Management Unit will conduct the review.

5. Other Related Procedures, Policies and Information Sources

5.1. Related Policies

- Data Protection – Manual of Guidance

5.2. Related Procedures

- N/A

5.3. Information Sources

- Data Protection Act 2018
- College of Policing APP – Information Management

Origin: Information Management