Data Protection Impact Assessment 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.

Overarching Policies:
Data Protection Policy

Procedures:
Information Sharing Procedure

Process

A Data Protection Impact Assessment (DPIA) is a tool that enables organisations that process personal data, including the Police, to identify the most effective way to comply with the requirements of the Data Protection Act and meet individuals' expectations of privacy. Data Protection Impact Assessments are a mandatory requirement under the Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR). A DPIA is required for any initiative where the processing of personal data could result in a high risk to the rights and freedoms of individuals. Initiatives could include the reuse of personal data we already use for other purposes, any new data sharing arrangements, any new system purchase, system replacement or alterations to systems containing personal data that could impact the personal data.

Early consideration of any risks posed to an individual's personal data supports the concept of Privacy by Design, which ensures that all Data Protection and privacy issues are considered from the earliest opportunity in an initiative's lifecycle. It is far easier to build privacy into a system at the development stage than trying to make something fit before go-live or even after go-live. If the need for a DPIA has been identified, **processing activity should not commence until the DPIA has been signed off**. Allowing processing to commence before the DPIA is completed could potentially result in high-risk processing and be in breach of data protection legislation.

North Yorkshire Police and the Police, Fire and Crime Commissioner will undertake a DPIA screening exercise (Appendix B) for all programmes, and initiatives where personal data is to be processed.

The screening exercise should be undertaken whenever we undertake the following:
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 cannot 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.

The DPIA screening exercise is embedded into regional and local procurement procedures, meaning that all requests for procurement, including renewals of existing contracts, will need to undergo the screening questions before any procurement work request will be accepted.

Prior to entering any information sharing arrangements, a DPIA screening questionnaire should be completed to identify whether a full DPIA is needed. Please see the Information Sharing Procedure.

To reiterate, if the need for a DPIA has been identified, **processing activity should not commence until the DPIA has been signed off**. Allowing processing to commence before the DPIA is completed could potentially result in high-risk processing and be in breach of data protection legislation.

As per the guidance available at Appendix A, this procedure will enable;

- The collection of sufficient information about a new process/initiative/IT system to allow a decision to be made as to whether a DPIA should be conducted;
- The decision as to whether or not a DPIA will be conducted.
- Any rationale as to why a DPIA has not been conducted to be recorded by the Information Management team.
- A DPIA to be conducted if required.
- Any privacy risks to be identified, documented, and considered, and effective, proportionate controls to be put in place within the DPIA; and
- Where a DPO has identified that the initiative is sufficiently high risk, a referral to the Information Commissioner will be completed by the relevant DPO to seek their view on whether the project/initiative should go ahead.

General Principles

- This procedure will assist staff to understand when a DPIA is necessary. A DPIA is not always necessary, there is no assumption that one must be done for every initiative. Where an extension to existing processing is proposed, which is already documented in a DPIA, the

Data Protection Team may ask that an annex or a shorter version of the DPIA is completed for the amendments only. This will then be appended to the existing DPIA.

- The DPIA should be started at an early stage when it can easily influence an initiative.
- Consultation is key; the focus should be on the identification of relevant stakeholders, and ensuring they are active and understand their role.
- The outcome of the consultation will allow for the identification of any privacy risks and the acceptance of any risk that is considered to be at an acceptable level.

Benefits

Undertaking a DPIA at the appropriate time will;

- Increase public confidence in the way in which North Yorkshire Police or the Police, Fire and Crime Commissioner collects and uses personal information.
- Allow the DPO to consider the legal basis for the new system, any obligation in relation to the collection of personal data and any prohibitions on the use of the information.
- Prevent problems from arising as the initiative progresses avoiding subsequent expense and disruption.
- Assist with risk management and facilitate the application of appropriate controls to protect the individual.

Timing of a DPIA

- A DPIA should be undertaken at the initial stage of any project or initiative, when we are considering reusing personal information that has been collected for alternative purposes, when making new policy on the processing of personal data and certainly before decisions are made about the processes to be implemented or systems to host the information.
- To be effective the DPIA should be reviewed regularly throughout each initiative phase and throughout the lifecycle of the processing.
- Retrospective DPIAs should not be undertaken.

Responsibilities

Overall accountability for ensuring a DPIA is completed rests with the Information Asset Owner (IAO).

The business lead will be responsible for ensuring that the DPIA is conducted at the earliest opportunity, and comprehensively completed following the DPIA guidance. The DPIA guidance is at Appendix C, the DPIA Stage 1 template is at Appendix D, the DPIA Stage 2 template is at Appendix E and the risk assessment matrix is at Appendix F. An absence of a DPIA when one is legally required can result in the processing being undertaken without sufficient safeguards to uphold individuals' rights and freedoms and may lead to enforcement action from the Regulator - the Information Commissioner's Office (ICO).

Consultation is an important part of the DPIA process and should be meaningful i.e. it should be designed as such that stakeholders can have a meaningful impact on the initiative. It allows stakeholders to highlight privacy risks based on their own area of interest and expertise. It also provides an opportunity for them to suggest measures to reduce the risks. It will allow the understanding of the concerns of those who will potentially be affected and will also improve transparency by making people aware of how information about them is being used. The timing and nature of consultation can be of particular importance if an initiative is sensitive.

Effective consultation should be:

- *Timely – at the right stage and allow enough time for responses*
- *Clear and proportionate – in scope and focuses*
- *Reach and representative – ensure those likely to be affected have a voice*
- *Ask objective questions and present realistic options*
- *Feedback – ensure that those participating get feedback at the end of the process.*

Consultation must take place with all relevant internal and external stakeholders, which may include the following: -

MUST CONSULT

- Data Protection Officer (DPO)
- Information Management including Information Security and Records Management

MAY CONSULT

- Risk and Assurance
- DISG
- Corporate Communications
- People Services
- Frontline staff / Officers
- Information Asset Owners
- Senior Information Risk Owner (SIRO)
- Legal Services
- Federation/Staff Associations
- Owner of other systems that are impacted upon
- Partner Agencies
- Data Processors (if used)
- Public (dependant on the information to be processed)
- Regulatory Authorities
- Information Commissioner – where it isn't possible to mitigate any high residual risks (to be completed by the DPO)

Once complete, the report will be submitted to the Data Protection Officer (dataprotectionofficer@northyorkshire.police.uk) for integration into the DPIA central register on The Source and Information Asset Register as appropriate.

Review of DPIAs

A DPIA should be reviewed periodically by the business lead, ideally annually, even if there have been no concerns with the processing of the data, to ensure that the DPIA accurately reflects the processing and the protections around the personal data.

A DPIA should also be reviewed whenever we are considering changes to the processing including the uses of the data, the access, the methods of collection, the storage, and the sharing of the data. Reviews may also be triggered by significant security incidents. The existing DPIA should be reviewed, consulted upon, amended, and approved as appropriate.