Data Protection - Safeguards for the Sensitive Processing of Personal Data Policy

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

Policy Statement

This policy statement is open to public viewing from the NYP Website.

The Data Protection Act 2018 (the DPA 2018), Section 35 (8) defines 'sensitive processing' as:

(a) the processing of personal data revealing racial or ethnic origin, political opinions, religious of philosophical beliefs or trade union membership;

(b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;

(c) the processing of data concerning health;

(d) the processing of data concerning an individual's sex life or sexual orientation.

Section 35 of the DPA 2018 states that data controllers should have an appropriate policy document (APD) in place that documents the safeguards in place for the sensitive processing that is used for law enforcement purposes, where the processing is reliant on consent or a condition specified in Schedule 8 of the DPA 2018.

When processing special category data under the General Data Protection Regulation (GDPR), the DPA 2018 Schedule 1, part 2, para 5, states that data controllers should have an appropriate policy document in place when relying on substantial public interest conditions.

This document will demonstrate that the processing of Special Category (SC) and Criminal Offence (CO) data based on these specific Schedule 1 and Schedule 8 conditions is compliant with the requirements of the Data Protection Principles.

Securing Compliance with the Data Protection Principles

NYP ensure compliance with the data protection principles by a number of avenues.

Accountability and Governance

We have a process within the organisation whereby a Data Protection Impact Assessment (DPIA) should be completed by relevant business areas when processing meets certain criteria (these mirror those criterion documented on the Information Commissioner's Office (ICO) website). This process is also embedded with the Regional Procurement Process as a screening checklist to demonstrate from the very start of a procurement exercise that a DPIA has either been considered and the procurement doesn't meet the DPIA criteria, or considered and is underway with consultation with the relevant stakeholder including the Data Protection Officer. The DPIA process and template identify any sensitive processing activities and look to put in place appropriate safeguards to protect this data. This includes implementing measures to achieve compliance with the principles and identifies the legal basis for the processing. The DPIAs are considered to be live documents and require periodic reviews.

Information Asset Owners (IAOs) have identified their information assets, and specifically those which contain sensitive processing, this is recorded on the Record of Processing Activities (RoPA). IAOs are required to complete bi-annual Assurance Statement for the Senior Information Risk Owner (SIRO) for each of their assets. The assurance statement contains questions that refer to the data protection principles and ask the IAO to provide evidence and assurances as to how they are ensuring compliance with these statements. Any concerns raised within these assurance statements are brought to the attention of relevant stakeholders, i.e. IAO, system owners, ICT, Information Security Officer, Records Manager, Data Protection Officer and the SIRO.

Although every employee in the organisation has a responsibility to ensure compliance with the data protection principles, there are key roles which take a more active role in the consultation, providing advice and input to ensuring compliance: the SIRO, the Data Protection Officer, the IAOs, the Information Management Lead, the Records Compliance Manager and the Information Security Officer. NYP also has an Information Assurance Board which is a board of relevant stakeholders in governing NYP's management of information.

Record of Processing Activities (RoPA)

This APD complements the record of processing created under Article 30 of the GDPR and provides SC and CO data with further protection and accountability. The RoPA is also the Information Asset Register, which is a record maintained and reviewed by IAOs annually (as part of their assurance statements). The record is maintained as and when DPIAs identify new processing or the re-use of personal data. The record documents the legal bases for processing of all personal data.

Lawfulness, fairness and transparency

We have identified an appropriate lawful basis for all processing undertaken and further Schedule 1 and Schedule 8 conditions for processing SC/CO data, as required. These are documented in the RoPA. We are also open and honest when we collect such data and ensure we do not deceive or mislead people about this, by providing suitable privacy notices on our website and via printed copies, if requested.

Purpose Limitation

We have we clearly identified our purpose(s) for processing the SC/CO data and have included appropriate details of these purposes in our privacy information for individuals. If we plan to use personal data for a new purpose (other than a legal obligation or function set out in law), we check that this is compatible with our original purpose or get specific consent for the new purpose, as required by the data protection legislation.

Data Minimisation

We are satisfied that we only collect SC/CO personal data we actually need for our specified purposes. We are satisfied that we have sufficient SC/CO data to properly fulfil those purposes and we periodically review this particular SC/CO data, and delete anything we don't need.

Data Accuracy

We have appropriate processes in place to check the accuracy of the SC/CO data we collect, and we record the source of that data, where appropriate. We have a process in place to identify when we need to keep the SC/CO data updated to properly fulfil our purpose, and we rectify or erase it as necessary without undue delay. We keep records of mistakes and opinions, distinguishing sensitive data processed based on fact from that based on opinion or assessment. We also deal with challenges to the accuracy of data and ensure compliance with the individual's right to rectification. Where appropriate we also distinguish between sensitive personal data relating to different categories of data subject and meet the verification requirements under section 38(5) for the transmission of data.

Storage Limitation

We carefully consider how long we keep the SC/CO data and we can justify this amount of time. We regularly review our information and erase or anonymise this SC/CO data when we no longer need it. Where a sustained need for continued retention of the information is identified, this is appropriately recorded and maintained. We have clearly identified any SC/CO data that we need to keep for public interest archiving, scientific or historical research, or statistical purposes and the appropriate data protection requirements are met where this applies.

Integrity and Confidentiality

We have analysed the risks presented by our processing and used this to assess the appropriate level of security we need for this data. We have an information security policy regarding this SC/CO data and we take steps to make sure the policy is implemented and regularly reviewed. Where appropriate, we have also put other technical measures or controls in place because of the circumstances and the type of SC/CO data we are processing.

Managing Consent

NYP has published to its internal intranet and to the website, our Consent Statement which sets out how we will manage consent including how we seek consent, how we should manage requests to withdraw consent and that we will conduct consent audits, as and when required.

Retention and Erasure

NYP maintains a retention schedule which serves as a policy document stipulating how long we should retain information, or even the criteria for retention, and the citation supporting the rationale. This is published on the internal intranet and on the website alongside our privacy notices.

When it is determined that the processing of special category data is no longer appropriate, we have active processes in place. The centrally based Review, Retention & Disposal team focuses on operational electronically held information in the principle recording system and the IAOs'

nominated individuals within their departments, to regularly manage the retention, deletion or restriction of their information across all systems within their area of responsibility.

In cases where it is not possible to delete or dispose in accordance with policies for example system constraints, we identify and apply measures to limit further processing.

Other Appropriate Safeguards in Place to Secure Compliance with Data Protection Principles

- Maintenance of an Information Risk Register
- Governance – Policies, Procedure, Guidance, Roles and Responsibilities, Information Assurance Board, reporting to SIRO
- Privacy Notice information (Privacy notice - North Yorkshire Police)
- Audit and training
- Data Processing Contracts
- Information Sharing Agreements
- Standard Operating Procedures
- Upholding Information Rights

Other Related Key Policies and Procedures
Records Management Policy
Information Security Policy
Data Protection Policy
Data Protection Impact Assessments Procedure
Review Retention & Disposal of Information Procedure
Retention Schedule
Consent Statement Guidance
Information Asset Register and Record of Processing Activity