Data Protection Policy

Version Record

Version No	Amendments Made	Authorisation
1	Draft / working copy by TLT Solicitors	Chief of Staff to the Chair of NPCC, December 2020
2	Revised version to reflect changes required by UK withdrawal from the EU and the implementation of the NPCC's Operating Model	Chair of NPCC 4th January 2022 at a meeting of the NPCC Command Team
2.1	Addition of NPCC Programmes as being subject to this policy (1.2) and addition of reference to PDS Acceptable Use Policy at 5.8	Strategic Hub Lead 21st February 2022

1 Introduction

1.1 The National Police Chiefs' Council (referred to in this policy as the **NPCC, we, us** or **our**) has established this policy to set out the key requirements with which we must comply to ensure compliance with the UK General Data Protection Regulation (**UK GDPR**) and the Data Protection Act 2018 (**DPA**). The NPCC is controller of personal data processed pursuant to its functions. The NPCC is also controller of personal data processed pursuant to the functions of the National Police Coordination Centre (**NPoCC**).

1.2 Where the NPCC processes personal data for any of the **law enforcement purposes** (defined at Section 31 of the DPA as - "the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security" – that processing must comply with Part 3 of the DPA. Where the processing is for any purpose other than the law enforcement purposes, referred to as for **general purposes**, the processing must comply with the UK GDPR as supplemented by the DPA. Collectively the UK GDPR and DPA are referred to as 'data protection legislation'.

1.3 This policy governs the way personal data is managed by police officers, staff members and contractors who work within NPCC Strategic Hub, NPoCC and the NPCC Programmes[1], or are based at NPCC's London HQ (referred to in the remainder of this policy as **staff, staff member** or **you**).

1.4 Although the NPCC is not a police force, we have a central role in assisting police forces by coordinating operations and the strategic direction of police work from a national perspective. In addition, we rely on the Metropolitan Police Service (the **MPS**) for a variety of underlying support services in its role as our host force.

1.5 To ensure alignment with the MPS' processes and the wider national policing information governance framework we have, where appropriate, taken account of the following when creating this policy:

1.5.1 the Authorised Professional Practice (**APP**) on Information Management published by the College of Policing https://www.app.college.police.uk/app-content/information-management), in particular the sections on:

(a) the management of police information (**MoPI**);

(b) sharing police information;

[1] These include Inclusion & Race, Violence Against Women & Girls and Office of the Chief Scientific Officer

(c) data protection;

1.5.2 various MPS policies covering information management matters such as the MPS Data Protection Policy; and

1.5.3 the NPCC Data Protection Manual of Guidance Version 2.0 July 2021 (available from the College of Policing's Knowledge Hub).

1.6 Although you may continue to be employed by your police force, please refer to this policy rather than the MPS Data Protection Policy in the first instance in respect of managing personal data in your role within NPCC Strategic Hub or NPoCC. This policy will help you understand which of the various documents referred to above at section 1.4 are relevant in relation each of our data protection processes.

1.7 This policy will help us to ensure that:

1.7.1 all staff understand their responsibilities in relation to data protection matters;

1.7.2 personal data is kept securely and is accessed only by those who need to see it;

1.7.3 individuals' rights are respected; and

1.7.4 appropriate controls are in place to ensure that use of personal data is necessary and proportionate.

1.8 We are supported with data protection advice by the NPCC Data Protection Officer (**our DPO**) and members of the NPCC's National Police Freedom and Information and Data Protection Unit (**NPFDU**) who include the NPCC Data Protection Advisor.

1.9 If you:

1.9.1 have any questions about this policy; or

1.9.2 are unsure as to how to deal with any personal data in a particular situation.

please contact our DPO by emailing dpo@npcc.police.uk rather than contacting the Information Commissioner's Office (**ICO**) or the Directorate of Legal Services (DLS) within MPS for advice.

2 Definitions

2.1 In the context of this policy the following definitions apply:

Criminal Offence data	Personal data that relates to an individual's criminal conviction or offence history
UK GDPR	UK General Data Protection Regulation
personal data	Information relating to an identified or identifiable living individual
personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data
process	Any operation or set of operations performed on personal data, including adapting, collecting, consulting, destroying, disclosing, erasing, organising, recording, retrieving, storing, structuring, and using
Special categories data	Personal data that: • Reveals an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership

- Relates to an individual's genetics and biometric profile processed for the purpose of uniquely identifying that individual; or
- Concerns an individual's health, sex life or sexual orientation.

3 Principles

The sections below set out the key principles with which all staff must comply to ensure that the processing of personal data is carried out fairly and lawfully, without adversely affecting the rights of individuals. Please refer to the APP guidance on data protection if you are still unsure on any of the key principles (the link to this is provided in paragraph 1.4.1 above).

3.1 1st Principle: Lawfulness, fairness and transparency

Requirement: Personal data must be processed lawfully, fairly and in a transparent manner.

3.1.1 What must we do to comply?

(a) Under the UK GDPR, we cannot process personal data unless one of the legal bases set out in the UK GDPR and/or (depending on the processing activity) the law enforcement purposes set out in Part 3 of the DPA apply. We must identify the legal basis and/or law enforcement purpose which permits data processing and record this in our central Records of Processing Activities.

(b) We must always balance our interests in using personal data against the privacy rights and expectations of individuals to ensure that use of personal data is fair but only where doing so would not prejudice law enforcement purposes in the context of law enforcement processing.

(c) We must ensure that individuals are provided with an easy to understand and easy to access explanation of how we will use their personal data at the point where personal data is collected, noting that processing, for a law enforcement purpose, this obligation may not apply or apply in a reduced capacity.

3.1.2 How do we ensure compliance?

(a) We maintain a central Records of Processing Activities (RoPA), in which the legal basis and/or law enforcement purpose of processing is identified for each processing activity. Our RoPA is managed by the DPO.

(b) When commencing new projects we carry out Data Protection Impact Assessments (DPIAs) to ensure that our use of personal data is necessary and proportionate and risks to personal data are appropriately mitigated.

(c) We maintain a Privacy Notice on our website, which explains how we process personal data about all categories of individuals whether for general processing or law enforcement processing.

(d) Your employing or host force should maintain internal facing privacy notices or policies which explain how it uses staff personal data in detail; these notices or documents also apply to the use of your personal data in the context of your work for the NPCC or NPoCC.

3.2 2nd Principle: Purpose limitation

Requirement: Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3.2.1 What must we do to comply?

(a) We must ensure that personal data is only used in accordance with clearly defined purposes for which it was collected and that, where appropriate and/or legally required, individuals have been notified of this purpose at the point of data collection.

(b) If any new use of personal data is proposed, we must carry out an assessment to ensure that the new use is compatible with the original notified purposes.

3.2.2 How do we ensure compliance?

(a) We have an NPCC Information Asset Ownership Policy which categorises each information asset we hold, including those which contain personal data, in relation to the purpose for which it was collected. The relevant Information Asset Owner has responsibility for ensuring personal data is used in a way that is consistent with that original purpose.

(b) We carry out regular audits of data processing activities to ensure that processing is consistent with the purposes notified to individuals.

(c) When commencing new projects we carry out Data Protection Impact Assessments (DPIAs) to ensure that any new use of personal data is compatible with the purposes notified to individuals. The template for recording DPIAs is available from the NPCC Data Protection Officer.

3.3 3rd Principle: Data minimisation

Requirement: Personal data must be adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed.

3.3.1 What must we do to comply?

(a) We must ensure that we only collect and use the minimum amount of personal data that is needed to achieve the purpose of processing.

(b) We must ensure that when it is appropriate to share personal data with third parties, only the minimum necessary personal data is shared.

3.3.2 How do we ensure compliance?

(a) The NPCC Information Asset Ownership Policy documents the hierarchy of responsibility for information assets, including those which contain personal data, within the NPCC Strategic Hub and NPoCC. The relevant Information Asset Owner shall be responsible for reviewing data collection points on a regular basis to ensure that only the minimum required amount of personal data is collected and used.

(b) When sharing personal data each staff member is responsible for ensuring that only the minimum amount of personal data is shared. If you have any questions or concerns about how much personal data to share in a particular situation, please contact our DPO.

(c) Our Risk Manager conducts reviews of data collection and data sharing activities on a regular basis to ensure data minimisation requirements are met.

3.4 4th Principle: Accuracy

Requirement: Personal data must be accurate and, where necessary, kept up-to-date. Every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified without undue delay.

3.4.1 What must we do to comply?

(a) We must put in place appropriate measures to check data accuracy by giving individuals an opportunity to review and update their personal data at regular intervals.

For law enforcement processing, as far as possible:

(i) a distinction must be made between personal data that is based on fact and that which is based on opinion or assessment; and

(ii) where relevant, a distinction is made between different categories of data subjects such as suspects, convicted persons, victims, witnesses and others.

(b) Where possible we should put in place appropriate tools to ensure accurate personal data is collected.

(c) If we are notified about inaccurate personal data (for example, a change of address), we must ensure that our records are updated promptly.

(d) An accurate record of an allegation, where the allegation is untrue, does not need to be amended if required for evidence.

3.4.2 How do we ensure compliance?

(a) All information is collected, recorded and evaluated in accordance with the APP on Information Management and this takes into account the obligations referenced at paragraph 3.4.1(a)(i) and 3.4.1(a)(ii).

(b) We have procedures in place for updating inaccurate or out-of-date records.

(c) We conduct regular reviews of our records to ensure that information assets are categorised and stored in accordance with our NPCC Information Asset Ownership Policy.

3.5 5th Principle: Storage Limitation

Requirement: Personal data must be kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the personal data is processed.

3.5.1 What must we do to comply?

(a) We must identify retention periods for personal data and ensure that personal data is either anonymised or securely destroyed or erased at the end of applicable retention periods.

3.5.2 How do we ensure compliance?

(a) We retain all personal data in compliance with the APP guidance on MoPI and we follow the MPS Records Management Policy including the Retention, Review and Disposal tables.

(b) Each staff member is responsible for ensuring that the APP guidance and MPS policy documents are followed in respect of their work.

(c) Our Risk Manager conducts reviews on a regular basis to ensure that the APP guidance and MPS policy documents are being followed.

3.6 6th Principle: Integrity and confidentiality

Requirement: Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

This requirement applies whether or not data subjects are otherwise identified or classified (by a police force or in legislation e.g. PACE) as a victim, witness, suspect, informant or a member of staff. This protection for personal data must always be applied equally both on an individual or collective basis.

3.6.1 What must we do to comply?

(a) We must put in place appropriate information security measures to protect personal data from unauthorised access, use, loss or disclosure.

(b) We must ensure that all staff understand the requirements of information security policies and comply with those policies.

3.6.2 How do we ensure compliance?

(a) All digital information under our control is stored on a secure server managed in-house by the MPS.

(b) Our systems containing digital information can only be accessed by vetted staff that have been appropriately authorised. Similar levels of access and security are applied to hard copy information held in our secure premises.

(c) We have an NPCC Information Code of Conduct in place which sets minimum standards for information security matters.

(d) Each staff member is responsible for ensuring that the NPCC Information Code of Conduct is followed.

(e) Annual training using the MPS Information & You training package is mandatory for all staff.

(f) Information Asset Owners ensure access to their records is restricted on a 'need to know' basis and that access is regularly reviewed.

3.7 Accountability

Requirement: We are responsible for, and must be able to demonstrate compliance with, the principles set out in sections 3.1 to 3.6 above.

3.7.1 What must we do to comply?

(a) We must ensure that appropriate policies and processes are in place to enable compliance with the data protection principles.

(b) We must monitor compliance with policies and processes and take action to ensure that any issues of non-compliance are remedied by the provision of further training or other measures.

(c) We must regularly review the adequacy of policies and processes to ensure they enable compliance with the data protection principles.

3.7.2 How do we ensure compliance?

(a) We have a number of policies and procedures in place governing how we process personal data in compliance with the data protection legislation as documented in this policy, which are listed at paragraph 6.

(b) We have a process in place to review all policies annually.

(c) The NPCC Data Protection Officer maintains a Register of Accountability Evidence for potential review by the Information Commissioner's Office.

3.8 Individuals' rights

Requirement: Under the UK GDPR and DPA individuals have the following rights:

- Right to be informed about how their personal data is used;
- Right to access personal data, however, it is subject to certain restrictions;
- Right to have inaccurate personal data rectified;
- Right to have personal data erased in certain circumstances;
- Right to restrict processing of personal data in certain circumstances;
- Right to data portability (which permits the individual to request a copy of personal data provided by the individual to us in a commonly used electronic format). This right does not apply to personal data processed for a law enforcement purpose;
- Right to object to processing of personal data in certain circumstances, including where personal data is used for marketing purposes, but only when it is not being processed for a law enforcement purpose; and
- Right not to be subject to automated decisions where the decision produces a legal effect or a similarly significant effect (such as deciding whether and on what terms to offer credit

to an individual) unless an exemption applies. We do not currently have any processes where the final decision is automated.

Please note, the above referenced rights only apply to living individuals.

Rights applications may be exercised verbally so should you receive one ensure that you record details of the application and evidence to prove the identity of the applicant. That information should then be forwarded to the NPFDU Data Protection Advisor.

If you ever receive an individuals' Rights Request (a **Request**) on behalf of a deceased person, for example in relation to specific incidents and the deceased individuals' involvement, you should refer the request to the NPFDU Data Protection Advisor.

You may also encounter requests in the form of a Freedom of Information Act 2000 (FoIA) request, which you should also refer to the NPFDU FoIA team.

3.8.1 What must we do to comply?

(a) We must put in place processes in order to ensure that when an individual wishes to exercise any of their rights under the DPA or UK GDPR the correct procedure is followed in order to respect those rights.

(b) Applications from individuals must be complied with without undue delay and, in any event, within one month from the date of request. Therefore, applications must be actioned promptly in accordance with the relevant procedure.

(c) All of our staff must be trained to ensure that they can recognise applications when they are raised.

3.8.2 How do we ensure compliance?

(a) Applications are handled in accordance with APP Information Management procedures by the NPFDU team.

(b) Personal Data for which the NPCC is a joint controller may be held by other police forces or policing bodies. Depending on the source and scope of an application, the NPFDU team will liaise with the Information Rights units and/or DPOs within the relevant police force or policing body to ascertain the most appropriate way to respond to an application.

(c) The NPFDU team will either:

(i) liaise with the Information Rights units and/or DPOs within police forces or policing bodies to collate the required information and respond to a Request directly; or

(ii) liaise with the Information Rights units and/or DPOs within police forces or policing bodies initially before passing the Request over to be dealt with.

(d) You will have undertaken mandatory foundation training on data protection matters, which includes training on individuals' rights. If you encounter a Request whether by post, email or any other medium, please refer it to the NPFDU team immediately.

(e) The NPFDU carries out regular reviews to check that statutory deadlines are being met and that Requests are being responded to in the correct manner.

3.9 Data Protection by Design and Data Protection by Default

Requirement: Taking into account the state of the art, costs of implementation, the nature of data processing and the risks to individuals, we must implement appropriate measures such as pseudonymisation which are designed to implement data protection principles.

3.9.1 What must we do to comply?

(a) We must consider when it is possible to pseudonymise or anonymise personal data.

(b) We must put in place measures to ensure that only the minimum level of personal data is collected and stored.

(c) We must ensure that when new projects are commenced data protection by design and by default principles are embedded in the project methodology from the outset.

(d) When procuring goods or services from third parties due diligence should be carried out to query how suppliers ensure data protection by design and by default.

3.9.2 How do we ensure compliance?

(a) At the start of new projects that involve personal data being processed and/or shared at a national level across multiple police forces we ask that the police force leading the project carries out a **DPIA** and consults with our DPO and/or NPFDU team in respect of data protection risk analysis. This ensures that data protection issues are considered from the outset so that data protection by design and by default is built into new processes and sharing arrangements. Please see paragraph 3.10.2(a) for details on how to find the NPCC DPIA template and guidance.

(b) Where we procure our own outsourced processing services (as opposed to relying on those sourced by the MPS), the appropriate staff will:

(i) carry out due diligence on new suppliers who will process personal data on our behalf to ensure they have measures in place to enable compliance with UK GDPR & DPA requirements;

(ii) be responsible for ensuring that all contracts with suppliers who process personal data contain the mandatory UK GDPR & DPA processing clauses;

(iii) carry out scheduled audits of suppliers to check compliance with contractual requirements

3.10 Data protection impact assessments

Requirement: If any data processing is likely to result in a high risk to individuals, police forces and policing bodies must ensure that a DPIA is carried out prior to beginning the processing. Our DPO and/or the NPFDU will be required to consult on DPIAs being undertaken by police forces embarking on new projects that involve high risk processing or sharing of personal data at a national level across multiple police forces, policing bodies or with external third parties.

Whether a project is high risk will depend on the potential risks to the individual and the intrusiveness of the processing being carried out. The DPIA must document the envisaged processing operations and the purposes of the processing, an assessment of the necessity and proportionality of the processing, an assessment of the risks to the individuals and the measures that will be taken to address those risks.

Where a proposed contract or procurement will lead to the processing of personal data the NPCC Data Protection Officer must be contacted for advice as to whether a DPIA is required.

3.10.1 What must we do to comply?

(a) We must put in place procedures to ensure that all new projects are assessed to determine whether there is any high risk data processing operation involved and, therefore, whether a data protection impact assessment is required.

(b) For all high risk processing we must assist police forces in ensuring that a DPIA is completed prior to the commencement of the processing.

(c) Our DPO and/or the NPFDU team must be consulted in relation to DPIAs that involve high risk processing or sharing of personal data at a national level across multiple police forces, policing bodies or with external third parties.

(d) We must ensure that the mitigating actions identified in a DPIA are implemented.

(e) If it is not possible to mitigate risks to stop them from being a high risk then it is necessary to consult with the Information Commissioner's Office. We therefore need to put in place procedures to escalate high risk projects where the risks cannot be mitigated to enable our DPO to consult with the Information Commissioner's Office as appropriate.

3.10.2 How do we ensure compliance?

(a) We have an NPCC DPIA Screening Questionnaire and DPIA template (with embedded guidance notes) which are available to NPCC and NPoCC staff and all police forces for use when embarking on project that involves the processing of personal data at across the national policing structure.

(b) Our DPO and the NPFDU team conduct engagement sessions and training to ensure that officers across the police service understand the importance of undertaking a DPIA when appropriate and how to go about using the NPCC DPIA Screening Questionnaire and DPIA template.

3.11 Record keeping

Requirement: We must keep a record of our data processing activities, including the name and contact details of the relevant company carrying out the processing, the purposes of processing, a description of the categories of individuals and categories of personal data, categories of recipients to whom personal data is disclosed, details of overseas data transfers outside of the UK or the European Economic Area, time limits for erasure of different categories of personal data and a general description of security measures in place to protect personal data.

3.11.1 What must we do to comply?

(a) We must ensure that a central record of all data processing activities is maintained.

(b) Any new data processing activities or changes to existing data processing activities must be recorded on the central record.

(c) We must put in place a process to regularly review the record to ensure that it is accurate and up to date.

3.11.2 How do we ensure compliance?

(a) We maintain a record of all data processing activities.

(b) Our DPO and Risk Manager are responsible for reviewing and updating the record annually and where there is a change in processing activities.

(c) Data Protection Impact Assessments are used to help identify when the record needs to be updated.

3.12 Engagement of external data processors

Requirement: We must only use processors that provide sufficient guarantees to implement appropriate measures to ensure that the requirements of UK GDPR, DPA. and the associated rights of individuals are met. In addition, arrangements with processors must be documented in a written contract and that contract must include mandatory clauses as set out in the UK GDPR or DPA. We must also carry out checks on processors to ensure that they are compliant with applicable requirements.

3.12.1 What must we do to comply?

(a) We must ensure that appropriate procedures are put in place to carry out due diligence on suppliers who will be processing personal data on our behalf to check that they have adequate measures in place to enable compliance with UK GDPR or DPA.

(b) All contracts with data processors must include our standard data processing provisions or equivalent provisions.

(c) We must put in place procedures to carry out ongoing monitoring of data processors to ensure compliance with data protection requirements.

3.12.2 How do we ensure compliance?

(a) We follow the APP on Information Sharing so staff should refer to this for general guidance on sharing personal data and the APP on Data Protection regarding appointing processors.

(b) We have developed a template for 'Data Processing Contracts' and the DPO is available to assist colleagues in the production of such contracts derived from the template.

(c) Where we procure our own outsourced processing services (as opposed to relying on those sourced by the MPS), the appropriate staff will:

(i) carry out due diligence on new suppliers who will process personal data on our behalf to ensure they have measures in place to enable compliance with UK GDPR or DPA requirements;

(ii) be responsible for ensuring that all contracts with suppliers who process personal data contain the mandatory UK GDPR or DPA processing clauses; and

(iii) carry out scheduled audits of suppliers to check compliance with contractual requirements.

3.13 Transfers of personal data outside the UK

Requirement: Personal data must not be transferred outside of the UK unless adequate protection is put in place for that personal data.

3.13.1 What must we do to comply?

(a) We must ensure that procedures are in place so that any transfers of personal data outside of the UK are identified prior to any transfer taking place and that a check is carried out to ensure that appropriate measures are in place to protect personal data.

3.13.2 How do we ensure compliance?

(a) Where any potential international data transfers are identified, staff must contact our DPO or the NPFDU team to ensure that adequate safeguards are, or already have been, put in place prior to any transfer occurring unless the transfer is made using a previously approved process that you may be aware of.

(b) Any transfers of personal data outside of the UK are documented in the Records of Processing Activities.

(c) Where third parties are engaged, our due diligence procedures require suppliers to notify us of any overseas transfers.

3.14 Breach notification

Requirement: If a personal data breach occurs we must notify the personal data breach to the Information Commissioner's Office unless it is unlikely to result in a risk to the rights and freedoms of individuals. If the breach could pose a high risk to individuals then those affected individuals must also be notified of the breach. Notification of the breach to the Information Commissioner's Office must take place within 72 hours of us becoming aware of the breach. Notification to individuals must happen without undue delay.

3.14.1 What must we do to comply?

(a) We must put in place procedures to ensure that as soon as any member of staff becomes aware of a personal data breach this is escalated to our DPO immediately.

(b) The DPO will review the nature of the breach, carry out an investigation and determine whether the breach needs to be notified to the regulator or to individuals.

(c) We must maintain a log of all personal data breaches and make this log available to the Information Commissioner's Office upon request.

3.14.2 How do we ensure compliance?

(a) We have an NPCC Data Breach Management Policy which explains what a personal data breach is and the procedure that must be followed if a personal data breach occurs. If you are ever unsure as to whether a breach has occurred and what action to take, please refer to this policy.

(b) Our DPO carries out regular reviews to ensure that the NPCC Data Breach Management Policy is being followed.

(c) Our DPO is responsible for maintaining a register of all personal data breaches irrespective of whether they have been reported to the Information Commissioner's Office.

3.15 Joint Controllership

Requirement: Where a controller jointly with others determines the purposes and means of the processing of personal data they and the other parties are considered to be joint controllers. Joint controllers must in a transparent manner determine their respective responsibilities for compliance with the UK GDPR and DPA. The arrangement must designate the controller which is to be the contact point for data subjects.

3.15.1 What must we do to comply?

We must identify all instances where we participate in joint controllership and ensure we in a transparent manner determine our respective responsibilities for compliance with the UK GDPR and DPA. We should document those respective responsibilities in writing in a Joint Controllership Agreement the contents of which may form part of a Collaboration Agreement under Section 22A of the Police Act 1996.

3.15.2 How do we ensure compliance?

(a) The Chief Constables' Council is currently determining the nature of joint controllership working involving their individual forces with the NPCC Strategic Hub, NPoCC, Co-ordination Committees, Portfolios and National Units. This analysis will inform the creation of any necessary Joint Controllership Agreements.

(b) Our DPO will assist in the creation and management of Joint Controllership Agreements involving the NPCC.

(c) Our DPO will carry out regular reviews of the NPCC's controllership arrangements and makes any necessary interventions.

3.16 Logging

Requirement: From May 2023 all databases processing personal data for law enforcement purposes must log the following: collection, alteration, consultation, disclosure, transfer, combination & erasure of personal data.

3.16.1 What must we do to comply?

We must identify all NPCC databases that process personal data for law enforcement purposes and ensure that by May 2023 they have the ability to log the collection, alteration, consultation, disclosure, transfer, combination & erasure of personal data. Any procurement of new databases to process for law enforcement purposes ensure the chosen product complies with this requirement.

3.16.2 How do we ensure compliance?

(d) Our DPO will review our Records of Processing Activities to identify any databases that need to satisfy the logging requirement.

(e) For each database that requires logging we will assess the extent to which existing logging satisfies this requirement and identify those where logs need to be enhanced or put in place

(f) The databases will be prioritised in order of sensitivity and a programme will be developed and implemented to create the necessary logging functionality.

(g) The logging requirement will be included in any user requirement for new NPCC databases that process personal data for law enforcement purposes.

3.17 Appropriate Policy Documents

Requirement: Appropriate Policy Documents are required to show the safeguards the NPCC has in place to protect special category data, criminal convictions data and where personal data is subject to sensitive processing for law enforcement purposes.

3.17.1 What must we do to comply?

We must have one Appropriate Policy Document for the processing of special category data and criminal convictions data, and another for sensitive processing for law enforcement purposes.

3.17.2 How do we ensure compliance?

(h) We have produced two Appropriate Policy Documents which are available from the Privacy Notice on NPCC's website.

3.18 Data Protection Offences

The DPA sets out criminal offences that may be committed by individuals. Those offences apply to both general processing and law enforcement processing. The offences are:

- breach of confidentiality by the Information Commissioner (DPA section 132).
- destroying or falsifying Information and documents etc. (DPA section 148).
- unlawful obtaining etc. of personal data (DPA section 170).
- re-identification of de-identified personal data (DPA section 171).
- alteration etc. of personal data to prevent disclosure to data subject (DPA section 173).
- enforced right of access (DPA section 184).
- The NPCC Data Protection Manual of Guidance has additional detail on all of the offences.

The offences of particular relevance to officers, staff and others working for the NPCC are examined in greater detail below.

3.18.1 Destroying or falsifying information and documents etc. (DPA section 148)

Where the Information Commissioner has issued an information notice or an assessment notice against the NPCC it is an offence to destroy or otherwise dispose of, conceal, block or (where relevant) falsify it, with the intention of preventing the Information Commissioner from viewing or being provided with or directed to it.

3.18.2 Unlawful obtaining etc. of personal data (DPA section 170)

It is an offence for a person knowingly or recklessly to obtain or disclose personal data without the consent of the controller (NPCC) or to procure the disclosure of personal data to another person without the consent of the controller (NPCC), or after obtaining personal data, to retain it without the consent of the person who was the controller in relation to the personal data when it was obtained.

3.18.3 Alteration etc. of personal data to prevent disclosure to data subject (DPA section 173)

It is an offence to alter personal data to prevent its disclosure following the exercise of a right of access or right to data portability application.

3.18.4 Enforced right of access (DPA section 184)

It is an offence for an employer to require employees or contractors, or for a person to require another person who provides goods, facilities or services, to provide certain records obtained via right of access applications as a condition of their employment or contract. It is also an offence for a provider of goods, facilities or services to the public to request such records from another as a condition for providing a service.

4 Accountabilities and Responsibilities

4.1 NPCC Chair:

4.1.1 Has ultimate responsibility for risk management, including setting risk culture and overseeing management's implementation of our strategy; and

4.1.2 Sets risk appetite and delegates authority for risk management.

4.2 Data Protection Officer:

4.2.1 Advises on obligations arising under data protection legislation;

4.2.2 Monitors compliance with data protection requirements, including legislative requirements and compliance with our policies;

4.2.3 Provides advice on Data Protection Impact Assessments and monitors performance of implementing actions identified in data protection impact assessments;

4.2.4 Has responsibility for liaising with the Information Commissioner's Office in relation to our data processing activities; and

4.2.5 Reports to the Chair of the NPCC on data protection compliance matters.

4.3 Strategic Planning & Risk Manager

4.3.1 Responsible for measuring, monitoring and controlling risks within NPCC Strategic Hub and NPoCC, in accordance with the Risk Management Framework.

4.4 Business Support Lead

4.4.1 Responsible for ensuring Business Support processes comply with this policy.

5 Related Policies and documents

5.1 NPCC Data Breach Management Policy

5.2 NPCC DPIA template and guidance

5.3 NPCC Information Asset Ownership policy

5.4 NPCC Information Code of Conduct

5.5 NPCC Data Protection Manual

5.6 NPCC Risk Management Framework

5.7 College of Policing Authorised Professional Practice on Information Management

5.8 Police Digital Service Acceptable Use Policy

6 Review of this policy

We will review this policy periodically and will make any updates deemed necessary. You will be required to comply with any updates made as from the date the updated policy is made available to all staff.

Any enquiries regarding this policy should be directed to its author, the NPCC Data Protection Officer, via dpo@npcc.police.uk