# Policy for the Processing of Special Category and Criminal Offence Data

| | |
|---|---|
| **Classification** | Internal |
| **Practice:** | East Norfolk Medical Practice |
| **Document Reference:** | ENMP Appropriate Policy Document (APD) |
| **Current Version Number:** | 1 |
| **Current Document Authorised By:** | Elaine Bond |
| **Current Document Approved By:** | Dr Inga Love and Jonathan Knights |
| **Date Approved:** | 14 December 2022 |
| **Review Date:** | 13 December 2022 |

| Version | Date | Version Created By: | Version Approved By: | Comments |
|---|---|---|---|---|
| 1 | 14/12/22 | Harriet Wilcox | Dr Inga Love,<br>Jonathan Knights | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# Policy for the Processing of Special Category and Criminal Offence Data

East Norfolk Medical Practice (ENMP) is committed to protecting the rights of individuals with regard to the processing of their personal data.

The function of the ENMP means it will frequently process special category data and criminal offence data in accordance with the requirements of Article 9 and 10 of the General Data Protection Regulation ('GDPR') and Schedule 1 of the Data Protection Act 2018 ('DPA 2018'). A requirement of processing these types of data require ENMP to have an Appropriate Policy Document ('APD') in place.

## Description of Data Processed

Special category data is defined at Article 9 GDPR as personal data revealing:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric data for the purpose of uniquely identifying a natural person;
- Data concerning health; or
- Data concerning a natural person's sex life or sexual orientation.

This document also refers to criminal conviction data. Article 10 GDPR covers processing in relation to criminal convictions and offences or related security measures. In addition, section 11(2) of the DPA 2018 specifically confirms that this includes personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing. This is collectively referred to as 'criminal offence data'

We also maintain a record of our processing activities in accordance with Article 30 of the GDPR.

## Schedule 1 Conditions for Processing

**Special Category Data (SC)**

We process SC data for the following purposes in Part 1 of Schedule 1:

- **Paragraph 1(1)** employment, social security and social protection.
- **Paragraph 6(1) and (2)(a)** statutory, etc. purposes

**Criminal Offence Data (CO)**

We process CO data for the following purposes in parts 1 and 2 of Schedule 1:

- **Paragraph 1** – employment, social security and social protection
- **Paragraph 6(2)(a)** – statutory, etc. purposes

## Procedures for ensuring compliance with the principles

When ENMP processes special category and/or criminal offence data under the conditions highlighted above, the processing is compliant against the principles under article 5 of the UK GDPR:

**Accountability principle**

We have put in place appropriate technical and organisational measures to meet the requirements of accountability. These include:

- The appointment of a data protection officer who reports directly to our highest management level.
- Taking a 'data protection by design and default' approach to our activities
- Maintaining documentation of our processing activities
- Adopting and implementing data protection policies and ensuring we have written contracts in place with our data processors
- Implementing appropriate security measures in relation to the personal data we process
- Carrying out data protection impact assessments for our high risk processing

We regularly review our accountability measures and update or amend them when required.

**Principle (a): lawfulness, fairness and transparency**

Processing personal data must be lawful, fair and transparent. It is only lawful if and to the extent it is based on law and either the data subject has given their consent for the processing, or the processing meets at least one of the conditions in Schedule 1.

We provide clear and transparent information about why we process personal data including our lawful basis for processing in our privacy notice, staff privacy notice and this policy document.

Our processing for the purposes of employment relates to our obligations as an employer.

**Principle (b): purpose limitation**

We will not process personal data for purposes incompatible with the original purpose it was collected for.

**Principle (c): data minimisation**

We collect personal data necessary for the relevant purposes and ensure it is not excessive. The information we process is necessary for and proportionate to our purposes. Where personal data is provided to us or obtained by us, but is not relevant to our stated purposes, we will erase it.

**Principle (d): accuracy**

Where we become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed, we will take every reasonable step to ensure that data is erased or rectified without delay. If we decide not to either erase or rectify it, for example because the lawful basis we rely on to process the data means these rights don't apply, we will document our decision.

**Principle (e): storage limitation**

All special category data processed by us for the purpose of employment is retained for the periods set out in our retention schedule. We determine the retention period for this data based on our legal obligations and the necessity of its retention for our business needs. Our retention schedule is reviewed regularly and updated when necessary.

**Principle (f): integrity and confidentiality (security)**

Electronic information is processed within our secure network. Hard copy information is processed in line with our security procedures.

Our electronic systems and physical storage have appropriate access controls applied.

The systems we use to process personal data allow us to erase or update personal data at any point in time where appropriate.

## Retention and erasure policies

Our retention and erasure practices are set out in our retention schedule.

## APD review date

This policy will be retained for the duration of our processing and for a minimum of 6 months after processing ceases.

This policy will be reviewed annually or revised more frequently if necessary.

For further information please contact Elaine Bond, Information Governance, Risk & Compliance Manager elaine.bond1@nh.net