



NORFOLK
CONSTABULARY



SUFFOLK
CONSTABULARY

DATA PROTECTION – PROCESSING SENSITIVE DATA (APPROPRIATE DOCUMENT)

Owning Department: Information Management

Department SPOC: Compliance and Data Protection Officer

Risk Rating: Low

Legal Sign Off: 10/03/2021

JNCC: March 2021

Published Date: 10/03/2021

Review Date: 19/09/2028

DATA PROTECTION – PROCESSING SENSITIVE DATA POLICY

Official

Index

1. Introduction.....	3
2. Applicability	4
Inclusions	4
Exclusions	4
3. Statement of Policy (Purpose).....	4
4. Compliance with data protection principles	4
a) 'Lawfulness, fairness and transparency'	4
Law Enforcement Processing	4
General Processing	5
b) 'Purpose limitation'	6
Law Enforcement Processing	6
General Processing	6
c) 'Data minimisation'	6
d) 'Accuracy'	7
e) 'Storage limitation'	7
f) 'Integrity and confidentiality'	7
5. Requirement to keep records of processing activity	8
Law Enforcement Processing.....	8
General Processing.....	8
6. Monitoring and Review	9
7. Guidance	9

Legal Basis

Legislation specific to the subject of this policy document:

- Data Protection Act 2018 – [Schedule 1 Part 4 and section 42](#)

Other relevant legislation which you must check this document against (required by law)

- [Human Rights Act 1998 \(in particular A.14 – Prohibition of discrimination\)](#)
- [Equality Act 2010](#)
- [Crime and Disorder Act 1998](#)
- [Health and Safety at Work etc. Act 1974 and associated Regulations](#)
- [Freedom Of Information Act 2000](#)
- [The Civil Contingencies Act 2004](#)

Other documentation which you must check this document against:

- [College of Policing – Code of Ethics](#)
- [Norfolk and Suffolk Constabularies' Standards of Professional Behaviour](#)
- [College of Policing – Authorised Professional Practice – Data Protection](#)
- Data Protection Policy
- Manual of Guidance for Data Protection Professionals
- Legislation/National Guidance
- Information Sharing Agreements

Official

Version Number: 1

Page 2 of 9

DATA PROTECTION – PROCESSING SENSITIVE DATA POLICY

Official

1. Introduction

- 1.1 This document is the 'Appropriate Document' which sets out how Norfolk and Suffolk Constabularies will protect special category personal data¹ and personal data relating to criminal convictions and offences, in compliance with Schedule 1 Part 4 and Section 42 of the Data Protection Act 2018 (DPA 2018).
- 1.2 Section 10 of the DPA 2018 requires that where the processing of special category personal data is reliant on one of the following lawful bases, as described in Article 9 of the General Data Protection Regulation 2016/679 (GDPR), the processing must also satisfy a condition in Schedule 1 of the DPA 2018.
- Article 9 (b) Employment, social security and social protection.
 - Article 9 (g) Substantial public interest.
 - Article 9 (h) Health and social care.
 - Article 9 (i) Public health.
 - Article 9 (j) Archiving, research and statistics.
- 1.3 Certain conditions within Schedule 1 DPA 2018 require that the Controller has an Appropriate Policy Document in place at the time the personal data is processed.
- 1.4 Section 35 (4) and (5) of the DPA 2018 require that where processing of personal data for any of the law enforcement purposes is sensitive processing, based either on the consent of the individual or condition within Schedule 8, the Controller shall have an Appropriate Policy Document in place.
- 1.5 The procedure provides 'high-level' direction and guidance to ensure compliance with the legal requirements of the Data Protection Act 2018 and UK GDPR². Further detail is available within the College of Policing's [Authorised Professional Practice \(APP\)](#) for [Data Protection](#) and the Manual of Guidance for Data Protection professionals.

¹Information relating to an individual's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life or sexual orientation

²UK GDPR means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 (and see section 205(4)

Official

Version Number: 1

Page 3 of 9

DATA PROTECTION – PROCESSING SENSITIVE DATA POLICY

Official

2. Applicability

Inclusions

- 2.1 This policy applies to (whether full-time or part-time), fixed term and permanent staff, seconded staff, temporary and agency staff, contractors, self-employed consultants and associates etc.

Exclusions

- 2.2 No known exclusions.

3. Statement of Policy (Purpose)

- 3.1 Where Norfolk and Suffolk Constabularies are carrying out the processing of special category and criminal offence data in its capacity as a Competent Authority and Controller, this document will explain:

- the procedures which are in place to secure compliance with the data protection principles set out in Article 5 of the GDPR and Section 35-40 of the DPA 2018
- when the processing is carried out in reliance on one of the conditions set out in Schedule 1, Parts 1-3; and;
- the policies about the retention and erasure of such personal data processed in reliance on a condition specified in Schedule 1 of the DPA 2018.

4. Compliance with data protection principles

a) 'Lawfulness, fairness and transparency'

Law Enforcement Processing

- 4.1 The lawfulness of sensitive processing, carried out by the Constabularies, is derived from its official functions as a public body and obligations or rights imposed or conferred by law as an employer.
- 4.2 The processing will be based either on the consent of the individual or that the processing is strictly necessary for the law enforcement purpose and meets at least one of the following conditions in Schedule 8 of the DPA 2018:
- Statutory Purposes
 - Administration of Justice
 - Protecting individual's vital interests
 - Safeguarding of Children and of Individuals at Risk
 - Personal data already in the public domain
 - Legal Claims

Official

Version Number: 1

Page 4 of 9

DATA PROTECTION – PROCESSING SENSITIVE DATA POLICY

Official

- Judicial Acts
- Preventing Fraud

General Processing

4.3 Where sensitive processing is carried out by the Constabularies for operational policing purposes that are NOT prescribed for under Part 3 of the DPA 18 (section 31: Law Enforcement Purpose) the processing will rely on one of the following lawful bases from Article 9 of the GDPR and will meet a relevant condition from Schedule 1 of the DPA 2018: -

- Article 9 (a) Consent
- Article 9 (c) Protecting vital interests
- Article 9 (e) Manifestly made public by the data subject
- Article 9 (f) Establishment, exercise or defence of legal claims
- Article 9 (g) Substantial public interest
 - Schedule 1, Part 2 (6): Statutory and government purposes;
 - Schedule 1, Part 2 (7): Administration of justice and parliamentary purposes;
 - Schedule 1, Part 2 (8): Equality of Opportunity or treatment;
Schedule 1, Part 2 (9): Racial and Ethnic diversity at senior levels of organisation;
 - Schedule 1, Part 2 (10): Preventing or detecting unlawful acts;
 - Schedule 1, Part 2 (11): Protecting the public against dishonesty;
 - Schedule 1, Part 2 (12): Regulatory requirements relating to unlawful acts and dishonesty;
 - Schedule 1, Part 2 (14): Preventing fraud;
 - Schedule 1, Part 2 (18): Safeguarding of children and of individuals at risk;
 - Schedule 1, Part 2 (19): Safeguarding of economic well-being of certain individuals;
- Article 9 (j) Archiving, research and statistics
 - Schedule 1, Part 1 (4): Research;

4.4 Where the processing of special category and criminal offence data is carried out by the Constabularies for non-operational policing purposes but predominantly as an employer, they will rely upon the following lawful bases from Article 9 of the GDPR and from Schedule 1 of the DPA 2018:

- Article 9 (a) Consent

Official

Version Number: 1

Page 5 of 9

DATA PROTECTION – PROCESSING SENSITIVE DATA POLICY

Official

- Article 9 (b) Employment, social security and social protection
 - Schedule 1, Part 1 (1): employment, social security and social protection;
- Article 9 (h) Health and social care
 - Schedule 1, Part 1 (2): Health or social care purposes;
- Article 9 (f) Establishment, exercise or defence of legal claims
- Article 9 (j) Archiving, research and statistics
 - Schedule 1, Part 1 (4): Research;

4.5 Further information is available to the public by accessing the Constabularies' high-level Privacy Notice available on the website at:

- Norfolk Information Charter
- Suffolk Information Charter

b) 'Purpose limitation'

Law Enforcement Processing

- 4.6 The Constabularies are authorised by law to process personal, special category and criminal offence data for any of the 'law enforcement' purposes. However, any further use of that data for a non 'law enforcement' purpose, under the GDPR, will only take place where it is authorised by law.
- 4.7 The Constabularies purpose for law enforcement processing are specified, explicit and legitimate, as well as necessary and proportionate. Where the Constabularies plan to use sensitive data for a new purpose other than that of law enforcement, the processing will comply with the requirements of DPA 2018 and GDPR.

General Processing

- 4.8 The Constabularies will only reuse personal, special category and criminal offence data collected under GDPR where that further use is compatible with the original purpose it was collected for.

c) 'Data minimisation'

- 4.9 The Constabularies only collects data that is necessary and proportionate to carry out its specified purpose. It is processed in the context of carrying out processes which enable the Constabularies to meet its stated policing or employment purposes for processing.
- 4.10 Additionally, the Constabularies' internal guidance, training and policies require staff to use only the minimum data required to achieve the specified purpose.

Official

Version Number: 1

Page 6 of 9

DATA PROTECTION – PROCESSING SENSITIVE DATA POLICY

Official

- 4.11 The Constabularies periodically review special category personal data and deletes data which is no longer required.

d) 'Accuracy'

- 4.12 It is the responsibility of the person who receives the original information to ensure, as far as it is possible, that it is accurate, valid and up to date.
- 4.13 Where processing personal data for law enforcement purposes a clear distinction must, where relevant and as far as possible be made between personal data relating to different categories of data subject such as suspects, convicted offenders, victims and witnesses or other persons with information about offences.
- 4.14 The development and procurement of Information Management systems will require that Privacy by "Design and Default" is embedded in such processes.
- 4.15 The Constabularies take reasonable steps to ensure that personal, special category and criminal offence data which is inaccurate, incomplete or out of date is not disclosed. If it is discovered, after disclosure, that the data was inaccurate, then the Constabularies will inform the recipient as soon as possible.
- 4.16 If an individual contacts the Constabularies regarding the accuracy of their data, it will respond to such requests in accordance with Article 16 of the GDPR/Section 46 data DPA 2018. Where it is decided not to erase or rectify the, the decision will be documented.
- 4.17 Requests for the disclosure of any personal information will only be considered once the Constabularies are fully satisfied that the enquirer or recipient is identified and authorised to receive the information.

e) 'Storage limitation'

- 4.18 Please find the link below for the Retention Schedule; applicable to retention of personal, special category and criminal offence data processed for a general purpose and law enforcement purpose.

Review, Retention and Disposal of Crime and Non-Crime Related Information - Schedule

- 4.19 Retention periods will be carefully considered for sensitive data and the purpose for which it is processed. A periodic review of retention periods will be undertaken to justify the need for retention of such data.

f) 'Integrity and confidentiality'

- 4.20 Section 2 of the GDPR and Sections 66-68 of the DPA 2018 contain the requirements for the security of personal data to include the implementation of appropriate technical and organisational measures to

Official

Version Number: 1

Page 7 of 9

DATA PROTECTION – PROCESSING SENSITIVE DATA POLICY

Official

include a level of security appropriate to the risks arising from the processing of personal data.

4.21 Appropriate technical and organisational security measures will include:

- Using and developing technological solutions to ensure compliance with the data protection legislation.
- Using and developing physical measures to protect force assets.
- Ensuring the reliability of any persons who have access to police information.
- Reporting and investigating security breaches.

4.22 These obligations include the need to consider the nature of the data to be protected and the harm that might arise from such unauthorised or unlawful processing, accidental loss, destruction or damage. The Government Security Classifications provide for such considerations and is adopted by the Force as part of its compliance with the NPCC Community Security Policy.

5. Requirement to keep records of processing activity

Law Enforcement Processing

5.1 Where the processing is sensitive processing the following information is recorded in our Record of Processing Activity:

- whether the sensitive processing is carried out in reliance on the consent of the data subject, or if not, which condition from the DPA 2018 Schedule 8 is relied on;
- how the processing satisfies Section 35 (lawfulness of processing); and
- whether the personal data is retained and erased in accordance with the policies described previously in this document, and, if it is not, the reasons for not following those policies.

General Processing

5.2 Where the processing of personal, special category and criminal offence data is carried out by the Force (as Controller) the following information is recorded in our Record of Processing Activity:

- whether the processing of personal, special category and criminal offence data is carried out in reliance on the consent of the data subject, or if not, which condition from the DPA 2018, Schedule 1 (Parts 1 and 2) is relied on;
- how the processing satisfies Article 6 and Article 9 of the GDPR (lawfulness of processing); and

Official

Version Number: 1

Page 8 of 9

DATA PROTECTION – PROCESSING SENSITIVE DATA POLICY

Official

- whether the personal, special category and criminal offence data is retained and erased in accordance with the policies described above in Section 3 of this document, and, if it is not, the reasons for not following those policies.

6. Monitoring and Review

- 6.1 The policy owner remains responsible for the monitoring of this policy throughout its lifespan, and is responsible for making any necessary amendments required due to changes in data protection legislation.

7. Guidance

- 7.1 If there are any queries in relation to the process of sensitive data, please get in contact with the Data Protection Officer via compliance@suffolk.police.uk
- 7.2 Further information around data protection requirements and the processing of data can be found in the Data Protection and Information Sharing policies.

Official

Version Number: 1

Page 9 of 9