DATA PROTECTION

Owning Department: Information Management

Department SPOC: Compliance and Data Protection Officer

Risk Rating: Medium High

Legal Sign Off: Alison Ings 12.11.24

JNCC: December 2024

Published Date: 16/12/2024

Review Date: 16/12/2027

Index

Legal Basis

Legislation specific to the subject of this policy document:

- Statutory Code of Practice for the Management of Police Information issued under The Police Act 1996
- Data Protection Act 2018
- Regulation of Investigatory Powers Act 2000
- UK General Data Protection Regulation
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988

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

- NPCC Data Protection Manual
- Authorised Professional Practice for Data Protection
- Authorised Professional Practice for Information Management
- Management of Police Information (MoPI) Statutory Code of Practice
- ICO Code of Practice on Data Sharing
- Acceptable Use of Information Systems and Assets Policy and Procedures

1. Statement of Policy

1.1 This policy has been formally agreed via the approved policy development/review process. It will be maintained by the Information Management Department in conjunction with the Central Policy Unit.

1.2 The policy is intended to promote equality, eliminate unlawful discrimination and actively promote good relations regardless of age, disability, gender reassignment, marriage or civil partnership, pregnancy and maternity, race, religion or belief, sex, sexual orientation, economic or family status.

1.3 Managers have a responsibility to ensure this policy is applied fairly, and unless otherwise stated, all policies and procedures are non-contractual.

2. Introduction

2.1 This policy applies to all officers, staff, volunteers and contractors working for Norfolk and Suffolk Constabularies.

2.2 This policy provides 'high-level' direction and guidance to ensure compliance with the Data Protection Act 2018 (DPA 2018) and UK General Data Protection Regulation (UK GDPR[1]). Further detail is available within the College of Policing's Authorised Professional Practice (APP) for Data Protection and the National Police Chiefs Council (NPCC) Data Protection Manual of Guidance for Data Protection Professionals.

2.3 This policy underwrites the commitment both forces have towards ensuring an individual's subject rights can be exercised in accordance with the DPA 2018 and UK GDPR.

2.4 Compliance with this policy is mandatory.

3. Governance

3.1 The Chief Constables of Norfolk and Suffolk Constabularies are the respective 'Controllers' as defined by the DPA 2018. They determine the purposes for which personal data is processed by the two forces and the

[1] UK 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)

manner in which that processing takes place. Both forces have appointed a 'Data Protection Officer (DPO)' and whose role and responsibilities are set out in the GDPR/ DPA 2018.

3.2 The respective Controller and relevant DPO contact details are below:

	Norfolk Constabulary	Suffolk Constabulary
Controller	Chief Constable Norfolk Constabulary Falconers Chase, Wymondham, Norfolk NR18 0WW Tel: 01953 425699	Chief Constable Suffolk Constabulary Police Headquarters, Portal Avenue, Martlesham Heath, Ipswich Suffolk IP5 3QS Tel: 01473 613500
Data Protection Officer	Compliance and Data Protection Officer Compliance@suffolk.police.uk	Compliance and Data Protection Officer Compliance@suffolk.police.uk

3.3 Notwithstanding that each Chief Constable remains a Controller in their own right, they have formally agreed how Controller responsibilities will be managed where collaborative activity is formally delivered through Section 22A Police Act 1996.

3.4 In addition to the roles of Controller and DPO, each force has appointed a Chief Officer to act as the Senior Information Risk Owner (SIRO). The SIRO has responsibility for sponsoring and promoting Information Management/Governance policy and overseeing compliance through a relevant force (joint) information management group.

3.5 The attendees at each Group include information management professionals and key internal stakeholders with senior leadership positions from across each organisation. Amongst these are individuals fulfilling the role of Information Asset Owner (IAO) who are key to ensuring compliance with the UK GDPR/ DPA 2018.

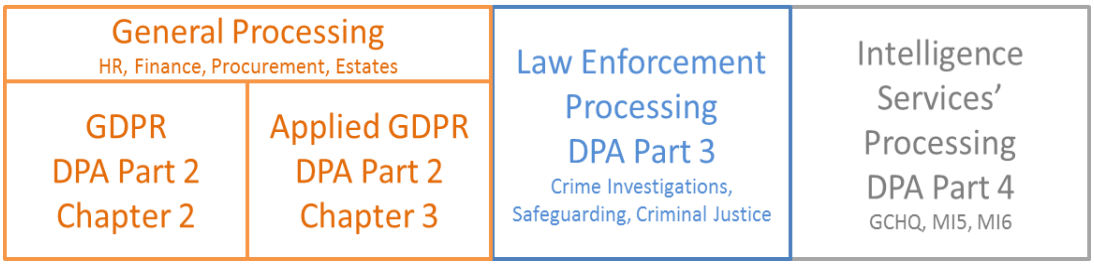
3.6 The IAO is a senior individual who holds relevant information responsibilities in relation to a particular business area. Their role is to oversee what information, including personal data, their staff collect, (physical and digital records), how it is used, what is added, what is removed, how information is transferred and who has access to it and why. As a result, they are able to understand and mitigate risks and provide assurance to the SIRO in relation to the security and accuracy of the force's information assets.

3.7 Information records are the corporate property of Norfolk and Suffolk Constabularies. Neither the physical record nor the intellectual information contained within either Norfolk or Suffolk Constabularies' records belongs to any particular group, team or individual.

4. Data Protection definition and principles

4.1 The Data Protection laws have been updated and incorporate two individual pieces of European legislation into the DPA 2018, namely the GDPR and Law Enforcement Directive (LED). Whilst the GDPR has direct effect across all EU member states, it also gives member states limited opportunities to make provisions for how it applies in their country. The details of which have been incorporated into one element of the UK DPA 2018. Following the UK leaving the EU, the GDPR forms part of law in the UK by virtue of the European Union (withdrawal) Act 2018. It is therefore important for practitioners to read the UK GDPR and DPA 2018 when determining and interpreting data protection law.

4.2 The below table helps to understand the legislative landscape:



4.3 ***Personal data*** means any information relating to an identified or identifiable living individual.

4.4 ***Identifiable living individual*** means a living individual who can be identified, directly or indirectly, in particular by reference to – (a) an identifier such as a name, an identification number, location data or an online identifier, or (b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

4.5 ***Data Subject*** means the identified or identifiable living individual to whom personal data relates.

4.6 All ***processing*** (which includes collection, recording, organising, structuring, storing, adaptation or alteration, retrieval, consultation or use, disclosure by transmission, dissemination or otherwise making available, alignment or combination or restriction, erasure or destruction obtaining, creating, amending, storing, disclosing, disposing) undertaken by Norfolk and Suffolk Constabularies will be in compliance with the Six Data Protection Principles relevant to the UK GDPR & DPA 2018 (Law Enforcement Part 3) subject to any legislative exemptions or restrictions. The principles, which differ according to whether the processing is for the Act (Law Enforcement purposes) or UK GDPR (General processing), are set out in the table below:

Law Enforcement Processing*	General Processing †
1st Principle - Processing of personal data must be lawful and fair	1st Principle – Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.
2nd Principle - Personal data collected on any occasion must be specified, explicit, and legitimate, and must not be processed in a manner that is incompatible with the purpose for which it was collected	2nd Principle – Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes
3rd Principle – Personal data processed for any purpose must be adequate, relevant and not excessive in relation to the purpose for which it is processed.	3rd Principle – Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)
4th Principle – Personal data processed for any purpose must be accurate and where necessary kept up to date and; every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified without delay. Fact and opinion must be clearly distinguished.	4th Principle – Personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
5th Principle – Personal data processed for any purpose must kept no longer than is necessary for the purpose for which it was processed. Appropriate time limits must be established for a periodic review of the need to continue to storage of the data.	5th Principle – Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals (Storage limitation)
6th Principle – Personal data processed for any purpose must be so processed in such a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures to	6th Principle – 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

protect against unauthorised, or unlawful processing and against accidental loss, destruction or damage.	appropriate technical or organisational measures.
In addition to the 6 principles above the DPA 2018 requires that the Controller is responsible for, and must be able to demonstrate, compliance with Chapter 2 (Principles and Safeguards) (Part 3 Section 34(3)).	In addition to the 6 principles above the law requires that the controller shall be responsible for, and be able to demonstrate, compliance with the principles. (Article 5(2))

*defined as the processing personal data for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and the prevention of threats to public security.

† defined as any processing of personal data not falling under the law enforcement processing i.e. HR, Finance, estates etc.

5. Legal Basis for Processing

5.1 For processing to be lawful under the 1st Principle, it must meet certain conditions set out in the DPA 2018 and UK GDPR.

5.2 For **Law Enforcement processing**, the law enforcement purpose has to be met in order to process personal data.

5.3 The law enforcement purpose is set out in Part 3 Chapter 1 Section 31 of the DPA 2018. It states the law enforcement purpose is processing for the purposes of the prevention, investigation, detection or prosecution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

5.4 When the law enforcement processing involves special category personal data, (information 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) one condition from Schedule 8 of the DPA 2018 must be met. The most relevant basis for policing are:

- necessary for judicial and statutory purposes – for reasons of substantial public interest;
- necessary for the administration of justice;
- necessary to protect the vital interests of the data subject or another individual.

5.5 For **General Processing**, one of the following conditions in Article 6(1) of the GDPR must be met for processing personal data. The most relevant ones are where:

- ***Consent***: the individual has given clear consent for the processing of their personal data for a specific purpose.

- ***Contract***: the processing is necessary for a contract the force has with the individual, or because they have asked the force to take specific steps before entering into a contract.
- ***Legal obligation***: the processing is necessary for the force to comply with the law (not including contractual obligations).
- ***Vital interests***: the processing is necessary to protect someone's life.
- ***Public task***: the processing is necessary for the force to perform a task in the public interest or for its official functions, and the task or function has a clear basis in law.

5.6 In addition, when the general processing involves special category data (information 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), one of the conditions under UK GDPR Article 9(2) or Schedule 1 Part 1 or 2 of the DPA 2018 must also be met. The most relevant ones are where:

- The individual has given explicit consent for the processing.
- The processing is necessary for lawful employment purposes.
- The processing is necessary to defend legal claims.
- The processing is necessary for reasons of substantial public interest
- The processing is necessary for occupational health purposes.
- The processing is necessary for archiving research and statistics purposes.

5.7 In order to process criminal conviction and offence data Article 10 of the UK GDPR and a condition from Schedule 1 Part 1, 2 or 3 has to be met unless the processing is carried out by a Competent Authority. Norfolk and Suffolk Constabularies are a Competent Authority as defined by Schedule 7 of the DPA 2018.

6. Subject Rights and the Responsibilities for officers and staff

6.1 Identifying Subject Rights Requests

6.2 Individuals are able to exercise eight rights concerning their personal data which is/has been processed by either force. The rights requests may be made verbally or in writing, and may be made directly to any officer or member of staff, or to the forces' specialist units which process all rights requests. A summary of the Subject Rights and which ones can be made verbally are as follows:

General Processing - GDPR and Part 2 DPA 2018	Law Enforcement Processing - Part 3 DPA 2018

Right to be informed (Articles 12,13,14) – Written	Right to be informed (S44) - Written
Right of access (Article 15) - Verbal/ Written	Right of access (S45) - Verbal/ Written
Right to rectification (Article 16) - Verbal/ Written	Right to rectification (S46) - Verbal/ Written
Right to erasure (Article 17) - Verbal/ Written	Right to erasure (S47) - Verbal/ Written
Right to restrict processing (Article 18) - Verbal/ Written	Right to restrict processing (S47) - Verbal/ Written
Right to data portability (Article 20) - Written	-
Right to object (Article 21) - Verbal/ Written	-
Rights related to automated decision making including profiling (Article 22) - Written	Rights related to -automated decision making including profiling (S49) - Written

6.3 All officers and staff must be able to recognise a subject rights application when one is made, and follow the processes set out in this section when receiving such a request.

6.4 Any failure to comply with these rights, or respond in a timely manner is likely to result in actions being taken by the regulator (Information Commissioner), including a potentially a significant monetary and/or reputational damage.

7. Rights in detail

7.1 **The Right to be Informed** - Individuals have the right to be informed about the collection and use of their personal data; we are obligated to provide individuals with information including: the purposes for processing their personal data, retention periods for that personal data, and who it will be shared with. This is referred to as 'privacy information'; which must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language. Information Asset Owners, working with the assistance of the (DPO), are responsible for ensuring this right is satisfied through the provision of privacy notices and/or Information Charter.

7.2 **The Right of Access (Subject Access)** - Individuals have the right to be aware of and verify the lawfulness of the processing the forces are carrying out. There is no requirement for a request to be in writing. We are required to provide a copy of the information free of charge, and at the latest within one month of receipt (subject to exemptions). All requests must be directed to the Data Protection Teams at the following address without delay: DataProtection@norfolk.police.uk or DataProtection@suffolk.police.uk. Both forces have application forms held on the forces' websites which applicants should be encouraged to utilise.

7.3 **The Right to Rectification** – Individuals have a right to have inaccurate personal data rectified or completed if it is incomplete. An individual can make a request for rectification verbally or in writing. The forces are obligated to provide a response within one calendar month. In certain circumstances the forces can refuse a request for rectification. All requests must be directed to the Compliance Team at the following address without delay: Compliance@suffolk.police.uk

7.4 **The Right to Erasure** – Individuals have the right to have personal data erased in certain circumstances. An individual can make a request verbally or in writing. All requests must be direct to the Compliance Team at the following address without delay: Compliance@suffolk.police.uk

7.5 **The Right to Restrict Processing** – Individuals have the right to request the restriction or suppression of their personal data. This is not an absolute right and only applies in certain circumstances. When processing is restricted, information is permitted to be stored but not allowed to be used. An individual can make a request verbally or in writing. All requests must be directed to the Compliance Team at the following address without delay: Compliance@suffolk.police.uk

7.6 **The Right to Data Portability (only applies to general processing)** - The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. All requests must be directed to the Data Protection Teams at the following address without delay DataProtection@norfolk.police.uk or DataProtection@suffolk.police.uk

7.7 **The Right to Object (only applies to General Processing)** - Individuals have the right to object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling). Also direct marketing (including profiling); and processing for purposes of scientific/historical research and statistics. All requests must be directed to the Compliance Team at the following address without delay: Compliance@suffolk.police.uk

7.8 **Rights related to Automated Decision Making including Profiling** – This right provides safeguards for individuals against the risk that a potentially damaging decision is taken by solely automated means, i.e. no human intervention. Currently, solely automated decision making that leads to an adverse outcome is rarely used in a law enforcement context and is unlikely to have many operational implications. All requests must be directed to the Compliance Team at the following address without delay: Compliance@suffolk.police.uk

7.9 **Actions to be taken by Officers and Staff in the event of a Rights request being exercised** - Any officer, member of staff or other individual working for or on behalf of either force must consider the following when they identify that an individual is attempting to exercise one of their Subject Rights:

- Take immediate steps to verify the identity of the person making the request, such as viewing a document such as a driving licence, passport etc., record the details of the request, and the method of identity verification, in their PNB or day book, and notify the relevant team, as outlined above, as soon as possible. If at all possible they should take a copy of the proof of identity.
- Where a request is initially made verbally officers and staff must write the request down and ask the requestor to verify the accuracy of their recording of it and amend it where necessary
- If the request is received by email, it must be forward to the relevant Data Protection or Compliance team ('team') as soon as possible, and they will deal with ID verification.
- If it is not possible to validate the individual's identity details of the request should be recorded and sent to the team. The individual should be guided to send documents to verify their identity to the team.
- You must notify the team as quickly as possible, as, subject to exemptions, they have only a month to respond fully. In this time they will have to search force systems, including in some instances paper records, to review their contents and send copies of the information to the individual requesting it.

8. Data Breaches and Responsibilities of Officers and Staff

8.1 A data breach is defined as a breach of information security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data transmitted, stored or otherwise processed.

8.2 All officers and staff have a responsibility to escalate any potential information security risks, or actual breaches as defined above, to their line manager immediately who must report the matter to Information Security in accordance with the Information Security Incident and Data Breach Reporting Policy.

8.3 Where the breach is of a significantly serious nature (to be judged by the DPO) it will be notified, as required by the DPA 2018, to the Information Commissioner's Office. Where a breach could seriously affect the psychological or the physical well-being of an individual, or individuals, whose personal data the Constabularies process, then this should be escalated as a potential critical incident to the Force Duty Officer who will instigate steps to contain the breach and notify the individual(s) concerned that a breach has occurred. Also to escalate the matter to either the Gold Commander and or DPO if appropriate.

9. Data Protection by Design and Default: Responsibilities for officers and staff.

9.1 The DPA 2018 places a legal obligation on the forces to consider data protection requirements at the earliest stage when developing new systems, IT applications and processes for handling personal data, including

information sharing initiatives – something known as Data Protection by Design and Default.

9.2 In some instances it will be necessary to carry out, with the assistance of the DPO, Data Protection Impact Assessments (DPIA) in accordance with NPCC Guidance. Please refer to the policy for Data Protection Impact Assessments

9.3 All officers and staff involved in projects or initiatives involving the use of personal data are required to make early contact with their DPO for guidance as to how the Data Protection by Design and Default requirements must be met.

10. Information Asset Register and Responsibilities of Information Asset Owners and Records Managers

10.1 To comply with the UK GDPR/ DPA 2018 each force will maintain an Information Asset Register (IAR) which will contain a comprehensive record of all of the information processed by the force, including the legal basis for processing, records of where consent is used, as well as the use of Information Sharing Agreements, Privacy Notices and retention periods.

10.2 The IAR will be managed by the Compliance Team, however it is the responsibility of Individual Information Asset Owners (IAOs) to ensure it is maintained, kept up to date by informing the Compliance Team of any new information and/or changes to existing information assets, as well as using the contents of the register to assess risk, direct interventions such as document reviews or weeding activity where retention periods being exceeded.

11. Controller and Processor Contractual Requirements and the Responsibilities of officer and staff

11.1 Both forces recognise that any third party whom processes personal data on behalf of one or both forces is within scope of the DPA 2018 and UK GDPR.

11.2 It is therefore a requirement of this procedure that any officer or member of staff who is responsible for entering into a new contract, maintaining an existing contract or entering into a procurement contract including the use of purchase orders must comply with Contract Standing Orders and the following mandatory process:

11.3 Consult with the DPO, to assess whether or not a DPIA is required.

11.4 Ensure that the contract has a viable Data Processing Contract/Agreement, or clause written into it that ensures that the Processor is clear on the Constabulary expectations of the method, security and legal obligations of their processing operation. Guidance can be sought from the Forces' Information Sharing Officer.

11.5 Ensure that the processing associated with the contract is fully documented on the force IAR, as well as the Record of Processing Activities, including an assessment of its risk.

11.6 Arrange for plans to be put in place to ensure that the Processor complies with the Data Processing Contract/Agreement using an audit programme. The frequency of audit will be dependent on the risk of the arrangement and data present.

11.7 In many circumstances it will be necessary to carry out a Data Protection DPIA. This is a statutory requirement, and where processing could present very high risk to data subjects may need to be submitted to and authorised by the Information Commissioners Office before the processing can proceed.

11.8 A DPIA template and guidance are available for both forces by contacting compliance@suffolk.police.uk

11.9 The procedure should not be regarded as an unnecessary bureaucratic burden. It applies a similar logic that used routinely within each force being no different to the thought process applied when using the National Decision Making Model (NDM), seeking Directed Surveillance authorities or completing an Equality Impact Assessment.

11.10 Copies of all DPIAs are retained centrally by the Compliance team and available to internal staff via the shared folder. They are also reflected on the IAR.

12. Retention and Disposal of Personal Data & Responsibilities of Information Asset Owners

12.1 Norfolk and Suffolk Constabularies review, retain and dispose of information in accordance with statutory and regulatory requirements and is directed through the application of the NPCC APP and the Management of Police Information (MoPI) Statutory Code of Practice

12.2 The retention, management and disposal of all physical and digital assets are the responsibility of the IAO, or the person delegated with that responsibility by the IAO.

12.3 All information assets must be managed securely and retained only as long as is necessary to meet the purpose for which they were collected and processed initially.

12.4 Further guidance on retention and disposal of personal data can be obtained from the Records Management and Data Quality Department and associated procedures.

13. Information Security

13.1 The Act requires both forces to ensure the 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.

13.2 Further guidance on the security of personal data can be obtained from the Information Security Unit and associated procedures.

14. Information Sharing

14.1 Information sharing involves the disclosure of data from one or more organisations to a third party organisation or organisations, or the sharing of data between different parts of an organisation.

14.2 Information sharing may occur on a formal basis, using express or implied powers as defined in statute, or on an ad hoc basis when for example dealing with an emergency or perhaps sharing data with a third party contractor to provide a specific service.

14.3 It is the policy of Norfolk and Suffolk Constabularies to follow the Code of Practice for Information Sharing published by the ICO. Additionally, when sharing information it is the responsibility of the IAO to:

14.4 Ensure that existing Information Sharing Agreements (ISA's) are current, kept up to date and are accurately reflected on the IAR/Central Record.

14.5 Ensure that when entering into a new ISA, consultation takes place with the DPO beforehand, and consideration is given to completing a DPIA.

14.6 That the contents of any privacy notice in use are consistent with the information contained within the ISA.

14.7 Further guidance can be obtained from the Information Sharing Team and associated procedures.

15. Transfer of personal data to Third Countries

15.1 The legislation imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations. These restrictions are in place to ensure that the level of protection of individuals afforded by the UK GDPR is not undermined. Personal data may only be transferred outside of the EU in compliance with the conditions for transfer set out in Part 3, Chapter 5 of the DPA 2018 and Articles 44 to 49 of the UK GDPR.

15.2 If an additional need arises to share personal data with third countries outside of the EEA, then the DPO must be consulted beforehand, and the principles as set out in Part 3, Chapter 5 of the DPA 2018 and Articles 44 to 49 of the UK GDPR adhered to.

16. Knowledge and skills

16.1 Both forces are committed to providing their officers, staff and volunteers with the appropriate level of skills and knowledge in data protection relative to the role they perform, and the data protection risks relative to that role.

16.2 Norfolk and Suffolk Constabularies share a single Learning and Development Department who are responsible for delivering Information Management Training using a national training product developed by the College of Policing.

17. Criminal Offences & Responsibilities of Officers and Staff

17.1 There are a number of criminal offences set out in the DPA 2018 which include:

17.2 **Section 170 Unlawful obtaining etc. of personal data** - It is an offence for a person knowingly or recklessly to obtain or disclose personal data without the consent of the controller, to procure the disclosure of personal data to another person without the consent of the controller, 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.

17.3 **Section 171 Re-identification of de-identified personal data** - It is an offence for a person knowingly or recklessly to amend information that previously could not identify a person so that the person can now be identified from it, without the consent of the controller responsible for anonymising the personal data in the first place.

17.4 **Section 173 Alteration etc. of personal data to prevent disclosure** - It is an offence for the controller or one of their employees to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information that the person making the request would have been entitled to receive having made a subject access request.

17.5 **Section 184 Prohibition of requirement to produce relevant records -** It is an offence for anyone offering employment, goods or services to someone else to compel the latter to provide them with, or give them access to the latter's personal data within records concerning a conviction, caution, health, or within a Disclosure & Barring Service record.

17.6 Where any of the above are suspected or identified officers and staff must:

- Record a criminal offence if appropriate in order that it can be assessed and allocated for investigation.
- Notify the DPO.
- If the offence relates to personal data processed by either force, report the matter to the Professional Standards Department.

- If the offence relates to personal data processed by either force, report the matter to the Professional Standards Department.
- If the offence relates to personal data processed by any other organisation, record the offence in accordance with crime recording policy and notify the DPO in order to consider onward referral to the Information Commissioner's Office.