POLICY

Data Protection

Policy Owner	Head of Information Management
Policy Holder	Information Compliance Manager
Author	Information Compliance Manager

Policy No.	4

Approved by

Legal Services	✓ 25.01.16.
Policy Owner	✓ 27.01.16.
JJNCC	✓ 04.01.16.

Note: *By signing the above you are authorising the policy for publication and are accepting responsibility for the policy on behalf of the Chief Constables.*

Publication date	02.02.16.
Review date	02.02.18.
APP Checked	N/A

Note: *Please send the original Policy with both signatures on it to the Norfolk CPU for the audit trail.*

Index

Legal Basis

(Please list below the relevant legislation which is the legal basis for this policy). You must update this list with changes in legislation that are relevant to this policy and hyperlink directly to the legislation.

Legislation/Law specific to the subject of this policy document

Section	***Act (title and year)***
	Statutory Code of Practice for the Management of Police Information issued under The Police Act 1996
	Data Protection – National Standard PNC Operating Rules
	Regulation of Investigatory Powers Act 2000
	Computer Misuse Act 1990
	Copyright, Designs and Patents Act 1988
	Data Protection Act 1998

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

Act (title and year)
Human Rights Act 1998 (in particular A.14 – Prohibition of discrimination)
Equality Act 2010
Crime and Disorder Act 1998
H&S legislation

Freedom Of Information Act 2000
Civil Contingencies Act 2004

Other Related Documents

- Authorised Professional Practice for Data Protection
- Authorised Professional Practice for Information Management
- Information Security Acceptable Usage Policy
- College of Policing Code of Ethics
- Norfolk and Suffolk Constabularies' Standards of Professional Behaviour
- ACPO Manual of Guidance for the Management of Police Information

1. Introduction

1.1 The Data Protection Act 1998 replaced the Data Protection Act 1984 in order to comply with a European Directive aimed at establishing standard practices across the EU on how personal data is processed, retained and stored.

1.2 This policy reflects current legislation and the requirements of the College of Policing Authorised Professional Practice APP for Data Protection. The day-to-day management of such matters will rest with the Information Compliance Manager and advice and decision making will be provided by the Data Protection Decision Maker. Should police officers or police staff require assistance or advice on any aspect contained within this policy, or any data protection issue, they should contact:

Data Protection Unit, OCC Wymondham

Ext: 2806/2807/3925

Data Protection Unit, Suffolk PHQ

Ext: 3514/3927

<u>Management of Police Information (MoPI) – statutory code of practice and manual of guidance</u>

1.3 Data Protection implementation and compliance are inextricably linked – MoPI is the police service practical implementation of the requirements of the Data Protection Act.

1.4 Whilst MoPI sets out procedural arrangements for the effective management of information, it does not provide the detailed legal interpretation of the Data Protection Act in the police environment. This document aims to provide that interpretation in the broad nature of police work and in some specific areas that commonly arise. Any issues not

covered in this document should be referred to the Data Protection Decision Maker for advice and guidance.

1.5 The Data Protection Act is applied to all personal data when processed by a Data Controller in electronic format (microfiche, image (moving and still) and email) and manual record.

1.6 Personal data is defined as information that can identify a living individual and other information which is in the possession of, or is likely to come into the possession of, the data controller. This includes the expression of an opinion about an individual and any indication of the intentions of the data controller or any other person in respect of the individual.

1.7 Processing is defined as any operation performed on the data, for example collecting, recording, viewing, retention, decision making, disclosure and destruction.

2. Data Protection Principles

2.1 This policy and the APP for Data Protection are based on the eight Principles within the Data Protection Act 1998. The Principles, which are summarised below, govern the holding of personal information and they provide the basis from which we can legally make use of the information. These Principles **must** be adhered to when processing personal data in any way.

2.2 The 8 Data Protection Principles are:

- Principle 1 – Personal data must be processed fairly and lawfully;
- Principle 2 – Personal data will be obtained only for lawful purposes;
- Principle 3 – Personal data will be adequate, relevant and not excessive for the purpose;
- Principle 4 – Personal data will be accurate and, where necessary, kept up to date;
- Principle 5 – Personal data will be held for no longer than is necessary for the purpose;
- Principle 6 – Personal data is to be processed in accordance with the rights of data subject;
- Principle 7 – Personal data will be subject to appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss, destruction or damage;
- Principle 8 – Personal data shall not be transferred to countries or territories outside the European Economic Area unless they ensure adequate levels of protection.

3. Principle 1

3.1 Personal data must be processed fairly and lawfully, and in accordance with at least one of the conditions in Schedule 2 of the Act. Where sensitive personal data is being processed, an additional condition from Schedule 3 of the Act must be adhered to.

3.2 Personal data will only be processed in compliance with the **'**policing purpose' as defined in the APP for Information Management:

- Protecting life and property
- Preserving order
- Preventing the commission of offences
- Bringing offenders to justice
- Any duty of responsibility of the police arising from common or statute law

3.3 The Constabularies will fulfil their fair processing obligations by informing data subjects of the following wherever and whenever it is practicable:

- Who the data controller is
- What personal data is being processed
- The purpose of the processing
- With whom information may be shared
- How they may obtain a copy of personal data that relates to them

3.4 The Constabularies will complete an annual registration/notification with the Information Commissioners Office.

3.5 The Constabularies will publish an Information Charter and Frequently Asked Questions on the website of the same information.

3.6 The Constabularies will detail a fair processing notice on forms that collect personal data whenever reasonably practicable.

3.7 Data subjects will be informed of the intended use and purpose of the processing of personal data when it may not be within their reasonable expectations. One particular example is where victim information is to be used to contact the individual in order to conduct a customer satisfaction survey. In these circumstances a letter is sent to the data subject informing them of the intention.

It has been confirmed by the Information Commissioner's Office (the Regulatory Body responsible for the Act) that it is not necessary for the police service to include a fair processing notice when receiving telephone calls via both the emergency and non-emergency numbers. Other parts of

the organisations that record calls should make members of the public aware as soon as the recording begins.

3.8 There will be occasions when informing the individual that information is held about them would not be appropriate, e.g. persons subject to investigations or operations, or intelligence records. The Act includes an exemption at Section 29(1) which states that where personal data is processed for the purpose of:

- The prevention or detection of crime;
- The apprehension or prosecution of offenders; or
- The assessment or collection of any tax or duty,

that processing is exempt from the requirement to produce a fair processing notice if to do so would or would be likely to prejudice any of those purposes. The Constabularies also makes a statement of exempt processing on the ICO registration.

4. Disclosure

4.1 Refer to the Information Sharing Policy and Common Law Police Disclosure Policy for further guidance relating to one off disclosures and systematic information sharing.

4.2 The disclosure of personal information is not covered by this Act alone; the Human Rights Act 1998 and common law duty of confidentiality as well as references in other legislation are also relevant. Guidance will be available from the relevant business area for the data in question and from the Data Protection Decision Maker. Guidance on specific subject matters is also available in the Information Sharing Arrangements:

- Suffolk Information Sharing Agreements
- Norfolk Information Sharing Agreements
- Joint Information Sharing Agreements
- National Information Sharing Agreements

4.3 The Data Protection Act 1998 includes some exemptions that allow for the disclosure of personal data:

- Section 29(3) – where disclosure is necessary for the prevention or detection of crime, or the apprehension or prosecution of offenders, and failing to disclose would prejudice those purposes;
- Section 35(1) – disclosure required under enactment, by any rule of law or by order of the Court;
- Section 35(2) – disclosure that is necessary for the purposes of legal proceedings.

Each of these exemptions still require that a condition for processing from Schedule 2 (& where necessary Schedule 3) is identified. The use of exemptions requires complex decision making and should be referred to the Data Protection Decision Maker where requests for disclosure are not routine.

4.3 Should an Officer or Police Staff member become aware of an Information Sharing Agreement and it is not recorded on the Central Repository or they have an idea for information sharing with a partner which is supported by their Manager, then the Officer/Staff must refer to the Information Sharing Policy and contact the Information Sharing Officer.

5. Principle 2

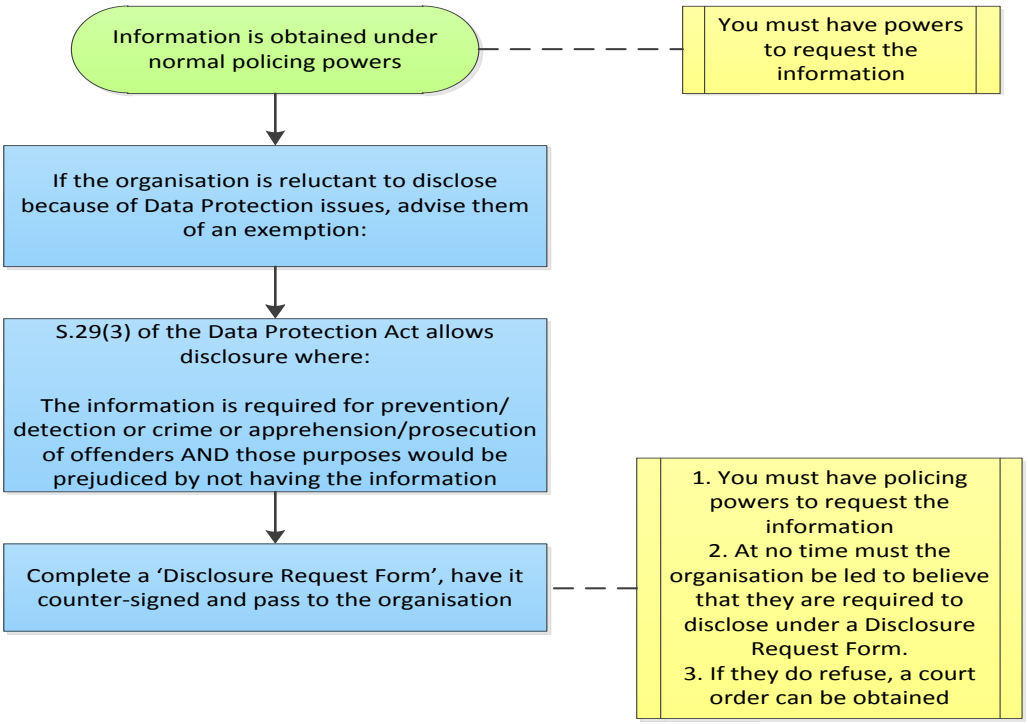
5.1 Personal data will be obtained only for **lawful purposes and not processed in a manner incompatible with those purposes**. This Principle ensures that organisations use only lawful methods in collecting and recording personal data.

5.2 When obtaining personal data from any source it is vital to be able to identify the source and validate the reliability of the information.

Some organisations, particularly private companies, may be concerned about providing personal data relating to an employee or a customer to the police for fear of breaching the Act. The following chart shows the options available to the police for providing support to external organisations in providing personal data for policing purposes.

In particular when officers are requesting medical or health information from a heath professional (or data from other organisations) to progress a criminal investigation it will be necessary for them to provide sufficient information to enable the health professional (or other organisation) to make a fully informed decision on whether to disclose information. The health professional (or other organisation) will not be obliged to make a disclosure but it is their decision to rely on the Section 29(3) exemption based on the information provided to them by the Officer. They may also charge for the service.

Points to remember when obtaining personal information from external organisations



NB. If a member of staff attempts or succeeds to obtain personal data by falsely stating that they have the necessary powers to do so, they will have committed a criminal offence under S.55(1) of the Data Protection Act 1998.

5.3 Principle 2 also relates to how information is used once it has been obtained, and in particular whether that use is in effect a change of purpose. A simple illustration of this is as follows:

- The police obtain and hold the name and address details of victims of burglary for the purpose of investigating and prosecuting the crime. We can also use that information to provide other policing services to the victim, such as referring them to Victim Support Services or offering crime prevention advice. If we were to use that information to invite the victims to a social event or pass their details to an organisation selling burglar alarms, that would be a change of purpose and incompatible with the original purpose for collecting the personal data.

6. Principles 3, 4 & 5

6.1 Personal data will be adequate, relevant and not excessive for the purpose.

Personal data will be accurate and, where necessary, kept up to date.

Personal data will be held for no longer than is necessary for the purpose.

These Principles can be referred to as the **data quality principles**.

6.2 Data Quality measures and controls are built-in to systems and business processes including training. However, data quality is the responsibility of all Officers and Staff. For further information please refer to the Data Quality Policy.

6.3 Information relating to the retention, review and disposal of information can be obtained from the Records Management department. It is important to note that Principle 5 is not a requirement to delete personal information; the requirement is to be able to justify its continued retention for a policing purpose.

6.4 If a member of the public wishes to complain about information held about them on police systems or in manual files, they can write to the Compliance Officer, Information Management Department. They should be advised to provide evidence of why they believe the data to be inaccurate. The Compliance Officer will consider their complaint and may amend or delete the data, add a statement to the data that the subject believes it to be inaccurate and why, or leave the data as recorded.

6.5 The public have a right to complain about any alleged breaches of the Data Protection Act to the Information Commissioner's Office.

7. Principle 6

7.1 Personal data is to be processed in accordance with the rights of data subject.

7.2 Principle 6 of the Act provides the following rights to the data subject:

- Right of access to their own personal data:
  - Subject Access – see below;
- Right to prevent processing:
  - On issue of a notice showing that processing would cause the subject substantial, unwarranted damage or distress;
- Right to prevent processing for the purpose of direct marketing (includes surveys):
  - Once notified, the data controller must take steps to ensure no future contact is made with the subject for this purpose;
- Rights in relation to automated decision-taking:
  - To be advised where a decision is based purely on automated methods;
  - To have that decision reviewed by means other than the automated process;
- Rights to compensation:

- For damage caused by the processing;
- For distress arising from the damage;

- Right to have inaccurate data rectified, blocked, erased or destroyed.

All correspondence received from data subjects, or their legal representatives on the above Rights is to be forwarded to the Compliance Officer, Information Management Department.

Subject Access

7.3 ALL subject access requests will be dealt with by the Data Protection Team. If you receive a verbal or written request from an individual wanting a copy of their personal data, refer this without delay to the Data Protection Decision Maker.

7.4 Subject Access requests fall into two categories:

- Information about criminal convictions held on the Police National Computer (or confirmation that there are none);
- Information held in the Constabularies records (e.g. domestic violence reports, crime reports, CAD reports, crime files etc).

NB. It should be noted that where a person is requesting a police check for the purpose of employment with or access to children or vulnerable adults they should be directed to the Disclosure and Barring Service.

NB. Where a person is requesting a police check for the purpose of obtaining a personal license under the Licensing Act 2003 they should be directed to either their local licensing authority or Disclosure Scotland for a basic check

7.5 Information about how to make such an application is held on each of the Constabularies external web-sites, including details relating to proof of identity. There are two forms via which a subject access application can be made:

- ACRO SAR1 for convictions information held on the Police National Computer;
- A221 (Norfolk) and 1091B (Suffolk) for all other information.

These forms can be found on the constabularies intranets.

The relevant Data Protection Office can be contacted on the phone extensions listed in section 1 of this document with any queries in relation to subject access.

A response to the applicant is required within 40 calendar days. The Data Protection Team will process all applications in accordance with the APP

for Data Protection and with reference to the Information Commissioners Office Subject Access Code of Practice.

8. Principle 7

8.1 Personal data will be subject to appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss, destruction or damage.

8.2 For further information please refer to the Information Security Policies, which address this element of compliance with the Act.

8.3 Under the Government Security Classifications, any system or document containing personal data is classified as "Official" or "Official – Sensitive Personal" and the appropriate storage, handling and transmission procedures will apply. For further information, refer to the Information Security Manager.

Data Processing Contracts

8.4 Where the Constabularies choose to employ the services of external organisations or individuals to carry out work on their behalf, which involves the use of personal data, a 'Data Processing' Contract is necessary to be put in place. Likely examples include:

- Hardware/Software suppliers and maintenance companies;
- Payroll suppliers;
- Confidential waste disposal contractors;
- Other persons (such as volunteers) working for the Constabularies;
- External organisations/auditors/researchers undertaking work on behalf of the Constabularies.

8.5 Any requirement for a Data Processing Contract must be referred to the Information Sharing Officer. Further information on Data Processing Contracts is available in the Data Processing Contracts Policy.

8.6 Guidance on specific subject matters is also available in the following paths:

- Suffolk Data Processing Contracts
- Norfolk Data Processing Contracts
- Joint Data Processing Contracts
- National Data Processing Contracts

9. Principle 8

9.1 Personal data shall not be transferred to countries or territories outside the European Economic Area (EEA) unless they ensure adequate levels of protection.

9.2 This restriction exists in the Act because this legislation was developed from a European Union Directive which requires all member states to produce domestic legislation that provides equivalent protection to personal data. Whilst other countries may have similar legislation it is only considered to afford the same level of protection as the Directive if it has been formally accepted by the Information Commissioner.

9.3 Schedule 4 of the Act provides conditions where a transfer of personal data to a country outside the EEA can occur. These include:

- With the consent of the data subject;
- In connection with legal proceedings;
- To protect the vital interests of the data subject;
- In the substantial public interest.

9.4 Any requirement to send personal data beyond the EEA, including contracts with companies who operate outside this boundary, must be referred to the Data Protection Decision Maker.

10. Compliance Management

10.1 The most effective way of achieving data protection compliance is through building compliance into systems, policies and procedures. This means that compliance is an integral part of the business process and not a side-issue or additional measure. Compliance can be achieved without placing any additional burden on resources. The following is a list of activities where early recognition of and consultation on data protection issues can ensure that compliance is built-in.

Activity	Data Protection Issue	Action & Resources
Introducing new system or software package	• Extent of personal data held • Data Quality • Data Retention • Disclosure • Access & permission levels • Printout & other disposable media • Subject access	The Communication Strategy and Project Initiation Document identifies key stakeholders to a new project. Information Management is listed on the Communication Strategy template as a key stakeholder for the Project Manager to contact. In some cases it will be necessary to conduct a

		Privacy Impact Assessment – the Project Manager or the Compliance Officer has access to the necessary resources and information. Produce Standard Operating Procedures for the management of the information and related business processes
Implementing new guidance or legislation Implementing new or changed business processes or procedures	• Notifying the public or staff of how their personal information will be affected • Recording methods • New or changed documents/forms	Contact the Compliance Officer In some cases it will be necessary to conduct a Privacy Impact Assessment – the Project Manager or the Compliance Officer has access to the necessary resources and information. Produce Standard Operating Procedures for the management of the information and related business processes
Developing or reviewing policy documents	• Fair and lawful use of personal data • Business process & procedures (see above)	Where a policy involves the collection and/or use of personal data, including staff information, include the Compliance Officer in consultation.
Information sharing arrangements with external organisations	• Fair and lawful use of personal data • Decision making on extent of disclosure • Legally binding agreements to reduce risk • Record keeping • Security	Consult the Information Sharing Agreement Policy. Contact the Information Sharing Officer.
Contracts	• Fair & lawful use of personal data • Legally binding agreement to reduce risk • Access & permission levels • Transfer of data outside EU	Contact the Procurement Officer. Contact the Compliance Officer.
Handling requests from individuals for their own personal information (including staff)	• Legal right to access • Managing rights within legal framework • Checking identity and charging appropriate fees	See subject access process above. Contact the Data Protection Decision Maker.
Handling requests from 3rd parties for personal	• Identifying access permitted by legislation	See guidance above on Disclosure.

data	• Use of appropriate exemptions • Consultation & consent • Recording decisions • Complaint handling	Contact the Data Protection Decision Maker.
Requesting personal information from external organisations	• What are the legal powers • Use of appropriate exemptions • Authority • Record keeping	Relevant form and instructions available
Handling complaints from the public and staff about the use of their personal information	• Recording complaints under Police Reform Act 2002 • Rights of redress under Data Protection Act • Criminal offences • Civil litigation	See guidance below.

11. Staff Training

11.1 Please refer to the Information Management Policy.

12. Monitoring and Audit

12.1 Please refer to the Information Management Policy.

13. Offences, Breaches and Investigations

Reporting and Lessons Learned

13.1 ALL suspected breaches of the Data Protection Act, including complaints against officers and members of police staff, will be notified to the Data Protection Unit. Notification can be done by Information Asset Owners, HR, supervisory officers, members of the Professional Standards Department or any member of the Constabularies who suspects a breach and/or offence might have occurred. If an officer or member of police staff receives an allegation from a member of the public that a Norfolk or Suffolk Constabulary employee has committed an offence under the Data Protection Act, this must be referred immediately to the Professional Standards Department.

13.2 Specifically when a Public Complaint has been received and/or Professional Standards/HR are investigating an alleged Criminal Investigation/Misconduct they will contact the Information Compliance Manager.

13.3 The Information Compliance Manager will carry out an initial assessment of the circumstances and provide advice on a range of issues including whether a criminal offence is likely to have been committed, and whether any further notification is required to the College of Policing and/or the Information Commissioner's Office. Details of the initial assessment

process are at Appendix A. The Head of Information Management and SIRO will be informed at the initial reporting, kept informed of progress and escalated to for the final decision making.

13.4 Professional Standards and HR will maintain contact with and provide updates to the Information Compliance Manager of the progress of the investigation and outcomes.

Breaches of the Data Protection Act and/or of Force Policy

13.5 **An organisational breach** relates to an activity that has been carried out in accordance with force policy and procedures, but where the policy and procedures are subsequently found to be in breach of the Act. An example would be, disclosing information under an agreed information sharing arrangement, which is ruled as being unlawful. Such breaches will usually come to attention via a complaint made to the Information Commissioner's Office (ICO). The ICO will conduct an assessment of the processing and determine whether or not the activity is compliant.

13.6 Norfolk and Suffolk Constabularies would then be required to take sufficient steps within a specified timeframe to prevent a reoccurrence. Failure to comply with either an Information or Enforcement Notice is a criminal offence.

13.7 **A personal breach** would be committed by an individual officer or member of police staff who have deliberately ignored or circumvented force policy and procedure, resulting in the Constabularies being in breach of the Data Protection Act. It is likely that any such action will be dealt with under the relevant disciplinary or performance procedures. An example of such a breach would be where a member of project, procurement or system owner staff has deliberately failed to notify the Data Protection Office of a contract involving access to Constabulary data by a private contractor and thus the appropriate safeguards and written agreements have not been put in place. Other examples may include, but are not limited to: Accidental or deliberate unauthorised destruction of information; Accidental or deliberate unauthorised modification of information.

Alleged Offences Identified by the Information Commissioner

13.8 Should the Information Commissioner receive allegations that the Constabularies or persons working for or on behalf of the Constabularies have committed offences under the Data Protection Act, the Information Commissioner will take primacy for the investigation and notify the Head of Professional Standards. Where the offender is a senior police officer of ACC or above, the Information Commissioner will notify the Police and Crime Commissioner.

Police Officers handling allegations of Criminal Offences under the Act Committed by Members of the Public or another Organisation

13.9 There are a number of criminal offences created by the Act as detailed above, with additional offences that can be referred to in the Act. Where a police officer receives a complaint that a member of the public or another organisation may have committed a criminal offence under the Data Protection Act, the Constabularies, in accordance with the National Crime Recording Standards and Associated Procedures, will record the allegation.

13.10 Where an allegation is made, the officer in the case will notify the case to the following:

The Head of Investigations
Information Commissioner's Office
Wycliffe house
Water Lane
Wilsmlow
Chesire
SK9 5AF

Telephone: 01625 545708

Email: investigations@ico.gsi.org.uk

13.11 Where the offence relates solely to data protection matters the Information Commissioner will deal with the investigation and prosecution.

13.12 Where a police officer discovers an offence has been committed whilst investigating another offence, e.g. fraud, it is important that all evidence relating to the data protection matter is secured and advice sought from the Information Commissioner to assist with the preparation of the case file for the data protection offences.

13.13 Where the circumstances of an offence committed under Section 55 of the Data Protection Act 1998 may also contribute an offence under the Official Secrets Act 1989, the police will investigate the matter and submit a file to the Director of Public Prosecutions.

14. Roles & Responsibilities

14.1 Please refer to the Information Management Strategy and Information Management Policy.

Appendix A – Data Protection Related Cases – Initial Assessment

1. Brief summary of circumstances as presented by complainant.
2. Description of information (what system, what records, manual or electronic, personal or non-personal data).
3. Is there prima facie evidence of an offence? Provide an explanation of your assessment, including what legislation applies.
4. Using the following points provide an assessment of proportionality – is the matter appropriate to pursue as a criminal offence, a disciplinary matter or words of advice?

    - The motive of the offender – was it a case of curiosity, was it for personal gain, was it for another person's gain;
    - The nature of the personal data – what quantity was involved, what it related to, its sensitivity, and so on;
    - Was the information accessed only, or also disclosed;
    - Was the access the result of a targeted search, general browsing or accidental as a result of a legitimate search;
    - Did the offender attempt to conceal their actions, e.g. using a wrong reference, using another's log-in. Did they raise the matter of inappropriate access/disclosure themselves;
    - The harm and/or distress, potential or otherwise, caused to the person to whom the personal data related and others;
    - The level of intrusion or breach of privacy suffered;
    - Previous misconduct or criminal breaches by the offender;
    - Whether the offender was one of many;
    - The wider public interest.

    Explain your assessment. Include any information about similar previous cases and CPS advice.
5. If the initial assessment is that criminal offences should be considered, provide any relevant guidance on the statutory defences and address issues such as training.