Lincolnshire
POLICE & CRIME COMMISSIONER
SAFER TOGETHER

DATA PROTECTION POLICY

Legislative Compliance

1. This document has been drafted to comply with the principles of the Human Rights Act. Proportionality has been identified as the key to Human Rights compliance, this means striking a fair balance between the rights of the individual and those of the rest of the community. There must be a reasonable relationship between the aim to be achieved and the means used.

2. Equality and Diversity issues have also been considered to ensure compliance with the Equality Act 2010 and meet our legal obligation in relation to the equality duty. In addition, Data Protection and Health and Safety Issues have been considered. Adherence to this policy or procedure will therefore ensure compliance with all relevant legislation and internal policies.

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

    - Human Rights Act 1998 (in particular A.14 – Prohibition of discrimination)
    - Equality Act 2010
    - H&S legislation
    - Data Protection Act 2018
    - General Data Protection Regulations (GDPR) (EU) 2016/679

Policy Aims (purpose)

4. The main aim of this policy is to ensure that personal information owned by the Office of the Police and Crime Commissioner (OPCC) is used appropriately in compliance with the requirements of the Act and that all officers and staff are clear about what is regarded as acceptable and what is improper use.

5. The policy is underpinned by procedure that sets out minimum standards and details how those employees and any other authorised person having access to any OPCC systems may use OPCC-owned personal information lawfully.

6. There are 6 Principles under GDPR and Data Protection Act 2018

    - Principle 1 – Lawful, Fair and Transparent
    - Principle 2 – Specified, explicit, legitimate
    - Principle 3 – Adequate, relevant and Limited to what is Necessary.
    - Principle 4 – Accurate, up to date
    - Principle 5 – Kept no longer than necessary
    - Principle 6 – Processed in a secure manner

Policy Statement: (Key information)

The principles and scope of the policy

7. The OPCC is committed to ensuring that all its officers, staff and contractors undertake their legitimate duties in a manner compatible with data protection principles set out in the General Data Protection Regulations (GDPR) (EU) 2016/679 and the Data Protection Act 2018 (herein after described throughout this policy as 'the Act').

8. The Act regulates the use of information from which a living individual can be identified. It applies to the processing of personal data in most formats including electronic, paper and other media.

9. A broad objective is to protect individuals from the use of inaccurate personal information, or misuse of accurate personal information. More specific associated objectives are to:

    a) ensure all persons having access understand their responsibilities regarding their use of personal information
    b) eradicate unlawful use of personal information
    c) safeguard all personal information
    d) protect the reputation of the OPCC by strict compliance with the Act and MOPI guidance

10. A right for an individual to access information held about them is provided by the General Data Protection Regulations (GDPR) (EU) 2016/679 and the Data Protection Act 2018.

11. All employees of the OPCC and those working voluntarily or under contract to the Police and Crime Commissioner (PCC) who have access to personal information must be aware of, and are required to comply with, all relevant policy and associated procedures.

12. This policy applies to persons at all levels of the organisation including all OPCC employees, temporary staff, agency staff, consultants, contractors and volunteer**s.**

13. The PCC will take criminal and/or disciplinary action against any category of person mentioned above whom wilfully accesses and/or misuses personal information held by the OPCC.

14. Any use of personal information that does not have a clear statutory or business purpose is likely to constitute a misuse. Using information is described as "processing" in the Act. See Part 1 3(4) of the Act that describes the ways in which data is defined as having been processed (used).

15. Part 6 Section 166 of the Act identifies the following criminal offence:

    A person must not knowingly or recklessly, without the consent:

    - obtain or disclose personal data or the information contained in the personal data, or
    - procure the disclosure to another person of the information contained in personal data.

16. The lead for this policy is the OPCC Corporate Administration Officer.

17. All employees of the OPCC and those working voluntarily or under contract to the PCC who have access to personal information must be aware of, and are required to comply with, all relevant policy and associated procedures.

Purpose

18. The OPCC needs to collect and use certain types of information about people with whom it deals in order to operate. These include current, past and prospective employees, suppliers and others with whom it communicates.

19. The OPCC may occasionally be required by law to collect and use certain types of information of this kind to comply with the requirements of government departments, for example ethnic monitoring of staff, or disclose personal information to comply with other legislation.

20. This personal information must be dealt with properly however it is collected, recorded and used – whether on paper, in a computer, or recorded on other material.

21. The lawful and correct treatment of personal information is regarded by the PCC as imperative to successful business operations, and to maintaining confidence between those with whom we deal and ourselves. The PCC needs to ensure that the organisation treats personal information lawfully and correctly.

Processing

Lawful Processing of Personal Data

22. The principal purpose for which the OPCC processes information is the administration of the OPCC and its employees.

23. Access to information systems or personal data including browsing, use or disclosure is permitted only to employees, contractors and approved persons working for or with the OPCC, where it is necessary in the course of their official duties.

24. The use of OPCC information systems for a private purpose or any other purpose other than that registered by the PCC to the Information Commissioner is prohibited.

25. Deliberate unauthorised access to, copying, destruction and/or alteration of, or interference with any computer or ancillary equipment or data (soft or hard copy) is an offence carrying a term of imprisonment under section 1 of the Computer Misuse Act 1990 and therefore strictly prohibited.

26. In order to meet the requirements for lawful processing, particular consideration will be given to:

    a) confidentiality arising from the relationship between the OPCC and any individual
    b) the ‘ultra vires’ rule and the rule relating to the excess of delegated powers, under which employees may only act within the limits of their legal powers;
    c) the legitimate expectations of any individuals in relation to the processing of information about them; and
    d) Article 8 of the European Convention on Human Rights (the right to respect for private and family life, home and correspondence).

Fair Processing

27. In meeting any obligation to ensure that processing of information is fair, due consideration will be given to the adoption of any recognised standards or advice to provide individuals with such information as is necessary to ensure that they are likely to understand:

    a) The purposes for which their personal data are to be processed
    b) The likely consequences of such processing; and
    c) Whether particular disclosures can reasonably be envisaged.

28. Chapter 2 of Part 3 describes the six data protection principles as follows –

    1. Requirement that processing be lawful and fair

    The processing of personal data for any of the law enforcement purposes must be lawful and fair.

    The processing is lawful only if and to the extent that it is based on law and either the data subject has given consent to the processing for that purpose, or the processing is necessary for the performance of a task carried out for that purpose by a competent authority (public task in the public interest).

    2. Requirement that purposes of processing be specified, explicit and legitimate

    The law enforcement purposes for which personal data is collected on any occasion must be specified, explicit and legitimate, and personal data so collected must not be processed in a manner that is incompatible with the purpose for which it was collected.

    3. Requirement that personal data be adequate, relevant and not excessive

    Must be adequate, relevant and not excessive in relation to the purpose for which it is processed.

    4. Requirement that personal data be accurate and kept up to date

    Personal data processed for any of the law enforcement purposes 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, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay.

    5. Requirement that personal data be kept for no longer than is necessary

    Please see the OPCC Review, Retention and Destruction Policy and Schedules:

    Policy: https://lincolnshire-pcc.gov.uk/media/1779/retention-and-disposal-policy-v21-feb-2018.pdf
    Schedules: https://lincolnshire-pcc.gov.uk/media/1778/schedules-v21-feb-2018.pdf

Requirement that personal data be processed in a secure manner

29. The OPCC will adhere to Lincolnshire Police Security Policy PD 55.

Sensitive Processing/Special Category Data

30. In this section, '*sensitive processing*' means:

    (a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
    (b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;
    (c) the processing of data concerning health;
    (d) the processing of data concerning an individual's sex life or sexual orientation.

31. Under GDPR (Part 2 of the DPA 2018) the OPCC will process data for General Processing Purposes in line with the conditions for lawful processing defined in Article 6 (1) of GDPR. Processing will be lawful if at least one of the following applies:

    6(a) The data subject has given consent to the processing for one or more specific purposes.

    6(b) Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

    6(c) Processing is necessary for compliance with legal obligation to which the controller is subject

    6(d) Processing is necessary in order to protect the vital interests of the data subject or of another natural person

    6(e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller includes processing of personal data that is necessary for

    (a) The administration of justice
    (b) The exercise of a function conferred on a person by an enactment.

    6(f) Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests of fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. (Point (f) shall not apply to processing carried out by public authorities in the performance of a public task).

<u>Special Categories of personal data</u>

32. The following subsections make provision about the processing of personal data described in Article 9(1) of the GDPR (prohibition on processing of special categories of personal data) in reliance on an exception in one of the following points of Article 9(2) -

    - point (b) (employment, social security and social protection)
    - point (g) (substantial public interest)
    - point (h) (health and social care)
    - point (i) (public health)
    - point (j) (archiving, research and statistics)

33. The processing meets the requirement in point (b), (h), (i) or (j) of Article 9(2) of the GDPR if it meets a condition in Part 1 of Schedule 1 of the DPA 2018.

34. The processing meets the requirement in point (g) of Article 9(2) of the GDPR if it meets a condition in Part 2 of Schedule 1 of the DPA 2018.

35. The processing meets the requirement in Article 10 (processing of personal data relating to criminal convictions and offences, etc.) of the GDPR if it meets a condition in Part 1, 2 or 3 of Schedule 1 of the DPA 2018.

36. The OPCC will only process special category data under Part 2 of the Data Protection Act 2018 when we have a lawful basis for doing so and the processing meets at least one of the necessary conditions in Schedule 1 of the DPA 2018. Additionally we will ensure that the Special Category Data is only kept for as long as is necessary, that being in accordance with our Review, Retention and Destruction policy and Schedules. Please refer for full details of retention periods.

Protecting the public against dishonesty, etc.

37. This condition is met if the processing –

    (a) is necessary for the exercise of a protective function;
    (b) must be carried out without the consent of the data subject so as not to prejudice the exercise of that function, and
    (c) is necessary for reasons of substantial public interest.

38. In this paragraph, 'protective function' – means a function which is intended to protect members of the public against –

    (a) dishonesty, malpractice or other seriously improper conduct;
    (b) unfitness or incompetence;
    (c) mismanagement in the administration of a body or association; or
    (d) failures in services provided by a body or association.

Data Protection Impact Assessments

39. To further support fair processing of Information, Data Protection Impact Assessments will be undertaken at the early stage of a project to help assess privacy risks to individuals in the collection, use and disclosure of information.

Registration

40. The National body for the supervision of Data Protection is the Information Commissioner to whom the PCC registers his purposes for processing personal data.

41. That registration process serves to provide transparency and openness about the processing of personal data. It is a fundamental principle of the Data Protection Act 2018 that the public should know, or be able to find out, who is carrying out the processing of personal data and for what purpose.

42. Copies of the PCC registration details are available upon request from the OPCC Corporate Administration Officer. It is also available on the Information Commissioner's Office website as www.ico.gov.uk

Disclosure

Personal Data

43. Information from OPCC information systems will, in the first instance, only be disclosed to employees who require such information in order to carry out their official duties. The information held is for OPCC use only but may in approved and established circumstances be supplied to other persons or organisations at the discretion of the OPCC.

44. Requests for the disclosure of any personal information will only be considered once the member of staff is fully satisfied that the enquirer or recipient is authorised to receive the information.

45. Care must be taken to ensure that any disclosure is within that allowed by any prevailing policy, guidance, Information Sharing Agreement, Memoranda of Understanding or statutory obligation or statutory provision and is authorised at the appropriate level.

46. Further specific advice and guidance concerning any aspect of information sharing or disclosure may be obtained from the Force Data Protection Supervisor and/or the Information Sharing Office within the Force Information Management Unit.

Live Data

47. To avoid any unintentional and/or unlawful disclosure, the use of 'Live' data held on computer systems or in manual filing systems for training, testing or practice purposes are strictly prohibited without prior and express consultation with the OPCC Chief Executive.

Subject Access and other Subject Rights

48. Article 15 of GDPR and section 43 of the DPA 2018 gives individuals the right of access to personal data held about them through the subject access provisions.

49. Through a subject access request, an individual is entitled to be:

- told whether any personal data is being processed;
- given a description of the personal data, the reasons it is being processed, an whether it will be given to any other organisations or people;
- given a copy of the personal data; and
- given details of the source of the data, where this is available.

50. The PCC acknowledges and adopts the Information Commissioner's Subject Access Code of Practice when processing subject access requests.

51. Where a subject access request is received by the OPCC, it will be dealt with in accordance with the Subject Access Code of Practice. Any person receiving such a request should direct it to the OPCC Corporate Administration Officer without delay.

52. **Appendix 1** provides further information on the administration and processing of subject access requests, as well as the Subject Access section on the PCC Internet site. **Appendix 2** is the Subject Access Form required for completion by the individual.

53. Under GDPR and Data Protection Act 2018 the individual has a number of additional rights which include Rectification, Erasure or Restriction of their information. If a request is received from an individual requesting any of these rights, the request should be forwarded to the OPCC Corporate Administration officer as soon as possible to allow this to be responded to appropriately.

54. The Corporate Administration Officer will use the following processes on how to assess and respond to these requests:-

    - **Appendix 3** – General Processing Rectification process
    - **Appendix 4** – General Processing Restriction process
    - **Appendix 5** – General Processing Erasure & Objection process

Data Integrity

Adequacy & Relevance

55. The reliability of information held in OPCC information systems depends primarily on the professional competence of staff who obtain and record information.

56. Information held on OPCC information systems must be adequate, i.e. fit for purpose, unambiguous and professionally worded.

57. Forms designed for the collection of information should only request that information which is pre-determined to be relevant in relation to the purpose for which it is required. Application forms should include a 'fair processing notice' where appropriate.

Accuracy

58. It is the responsibility of the person who receives the original information to ensure, as far as is possible, that it is accurate, valid, and up-to-date.

59. All staff should ensure that all information entered on OPCC records is adequate, relevant, unambiguous and professionally worded. Where errors are found on any personal information held they will be reported to the appropriate line manager and corrected at the earliest opportunity.

60. Cancellations, amendments and deletions should be carried out as a matter of priority. However, in order to retain the OPCC's corporate memory of our interaction with the person(s) concerned if inaccurate personal information is found and subsequently corrected consideration must be given to retaining the original information, with an appropriate entry being made to direct all future users of that information to the corrected data.

61. Where it is known that inaccurate information may have been disclosed to a third party, the corrected information should be disclosed to that party with explanation, together with any other action necessary to minimize any harm, loss or damage arising from such disclosure.

Review, Retention and Disposal of data

62. Unless a system incorporates automatic facilities or other structured procedures, reviews of personal data must be carried out at frequent intervals to ensure immediate cancellation or amendment of unneeded or out-of-date material. This is good practice that should be applied to all information held for OPCC purposes.

63. The Review, Retention and Disposal Policy and Schedules, and other legal requirements for the retention of documents, should be referred to for further guidance on this subject.

Information Security

64. The GDPR Sixth Principle – Integrity & Confidentiality (GDPR Article 5) requires that appropriate technical and organisational measures shall be taken to protect data against:

    (a) unauthorised access
    (b) unauthorised or unlawful processing
    (c) accidental loss, destruction or damage

65. Appropriate technical and organisational security measures include:

    - using and developing technological solutions to ensure compliance with the data protection principles
    - using and developing physical measures to protect OPCC assets
    - ensuring the reliability of any persons who access OPCC information
    - reporting and investigating security breaches

66. 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 or accidental loss, destruction or damage. The Government Protective Marking Scheme and Government Security Classification Scheme provide for such considerations and are adopted by the OPCC.

67. All printout material, magnetic tape, diskettes, CD's or DVD's, manual files, handwritten notes, etc., which contain personal data and are no longer required, should be treated as confidential waste and disposed of in accordance with Lincolnshire Police Security Policy (PD55).

68. Good information security is also achieved through policy and procedural controls, details of which are documented in the Lincolnshire Police Security Policy.

Third Party Processing

69. Where processing of OPCC data is to be carried out by a third party on behalf of the OPCC, the PCC must ensure that party provides sufficient guarantees in respect of the technical and organisational measures governing the processing to be undertaken.

70. This means that appropriate contractual terms and conditions will be imposed on any third party data processor to ensure that they act only on instructions given by the PCC in regard to that processing.

71. The processing must be deemed necessary and approved by the OPCC Chief Executive and a designated Manager will be appointed to assume responsibility for the arrangements. Where such processing is approved, it may be necessary to consult and seek advice from the Force Data Protection Officer.

72. Where financial consideration is in connection with any procurement of services, the Head of Force Procurement must be advised in order that the OPCC's obligations for procurement are also met. All relevant information is contained within the Data Handling Schedule that is part of the procurement process.

Bulk Data Transfer

73. Where a significant volume of data identifying individuals is to be transferred outside of the OPCC, either electronically or manually, in a single instance, it is the responsibility of the member of staff to consult with the Force Security Officer or the Data Protection and FOI Manager for advice and guidance regarding data protection requirements.

Data Security Breach Management

74. When a breach of data protection for personal data occurs this needs to be reported to the OPCC Chief Executive and Force Security Officer as soon as possible along with the appropriate completed Security Incident form (P755). This will then be forwarded to the Force Data Protection Officer for notification to the ICO (within 72 hours) if necessary. **Appendices 6 and 7** to this policy provide the process for breach reporting.

75. Good information security is also achieved through policy and procedural controls such as the OPCC's Clear Desk Policy and the Government Security Classification Scheme.

Data Protection Impact Assessments (DPIA)

76. Data protection impact assessments (also known as privacy impact assessments or PIAs) are tools which can help organisations identify and minimise the Data Protection risks of a project, new system or process. You should consider carrying out a DPIA in any major project involving the use of personal data. You should carry out a new DPIA if there is a change to the nature, scope, context or purposes of our processing.

77. An effective DPIA will allow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur. To assess the level of risk, you must consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm

78. If the OPCC is introducing a new process / initiative or IT system or is making significant changes to a process / IT system, that has implications for the use of personal information, a DPIA should be assessed according to the below criteria.

79. Initial DPIA work should be undertaken prior to going to tender (i.e. at project initiation phase or its equivalent or the business case stage – certainly before decisions are made about the IT system / process / initiative). It may be appropriate to insert the initial DPIA within a relevant contract.

80. We should always carry out a DPIA if we plan to:

- use systematic and extensive profiling or automated decision-making to make significant decisions about people
- process special category data on a large scale
- systematically monitor a publicly accessible place on a large scale
- use new technologies
- use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit
- carry out profiling on a large scale
- combine, compare or match data from multiple sources
- process personal data without providing a privacy notice directly to the individual
- process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them
- process personal data which could result in a risk of physical harm in the event of a security breach

81. We should consider carrying out a DPIA if we plan to carry out any other:

- evaluation or scoring
- automated decision-making with significant effects
- systematic Processing of sensitive data or data of a highly personal nature
- processing on a large scale
- processing of data concerning vulnerable data subjects
- innovative technological or organisational solutions
- processing involving preventing data subjects from exercising a right or using a service or contract

82. If you decide not to carry out a DPIA, you should document your reasons.

83. More information on DPIAs is contained in the Lincolnshire Police DPIA Policy PD 170.

OPCC Systems

Design and Development

84. It is the responsibility of the OPCC and specialists responsible for the development or alteration of systems or databases to ensure that appropriate consultation takes place between the User, the Lincolnshire Police Information Management Unit, Force Security Officer and IT Security Officer to ensure compliance with the relevant statutory provisions including:

(a) Data Protection Act 2018
(b) The Computer Misuse Act 1990
(c) The Copyright, Designs and Patents Act 1988
(d) The Official Secrets Acts
(e) General Data Protection Regulation (EU) 2016/679 (GDPR)

85. The development of new systems provides an opportunity to build in data protection compliance at the time of the design by providing security against any breaches of the Act by considering:

- The state of the technological development to include privacy advancing technology
- The nature of the data to be protected
- The harm that might result from a breach of security
- Any likely impact on privacy

86. The Force Data Protection and FOI Manager and Data Protection Supervisor will assist the OPCC in considering data protection requirements to include the undertaking of Data Protection Impact Assessments to assess and identify any privacy concerns, as well as the consideration of appropriate privacy enhancing technologies to achieve compliance.

87. Failure to meet these requirements may lead to costly software amendments, unnecessary delays or the postponement of implementation.

88. Further advice and guidance is available from the Force IT Security Officer and Force Security Officer.

Audit and Monitoring

89. In order to ensure compliance with the Data Protection Act 2018, GDPR and other relevant standards for the management of information, the PCC is obliged to have an audit regime to measure performance to comply with legislative and policy requirements and thereby help in endorsing the effectiveness and efficiency of OPCC policies.

90. The purpose of an audit is to provide a systematic and independent examination to determine whether activities involving the processing of OPCC information are carried out in accordance with the organisation's policies and procedures and whether this processing meets the requirements of relevant legislation and standards.

91. A Central Audit Schedule will be developed from comprehensive risk analysis in accordance with the framework and standards provided by the Data Protection Audit Manual (Office of the Information Commissioner June 2001).

92. This will determine the nature and scope of the audit, taking into account available resources and provide a strategy which will form the basis of audit activity for the period under consideration. This Schedule will be subject to annual review and lead to a documented Audit Plan which will outline:

    - Areas to be audited
    - Target dates
    - Resource allocation

93. It is recognised that limited resources may restrict the number of applications or systems, which may be audited. However, the decision regarding which applications or systems will be audited, and the scope and frequency of such audit will be subject to a formal risk assessment process and current business needs.

94. Individual audits (as specified in the Schedule) will be subject to a separate planning process, with the aim of performing the audit in an effective and efficient manner. The audit plan will set out the following:

- the scope and objectives of the audit
- conduct/methodology of the audit
- classification error criteria
- resource allocation and target timescales

95. The audit programme will be supplemented by quality assurance and monitoring processes undertaken in each area of OPCC business.

96. Transaction checks will also be carried out on a regular basis in order:

    - to deter and detect unauthorised access to police information or systems
    - to raise staff awareness of data protection issues, and maintain public confidence in the use of OPCC information
    - to ensure that all required transaction fields are completed to provide an adequate audit trail for retrospective investigations into transactions that has been carried out

Roles & Responsibilities

Data Controller

97. The Data Controller is the person who determines the purposes for which, and the manner in which, any personal is processed. The PCC is the Data Controller for the OPCC.

Data Protection Officer

98. This is a statutory duty, which for the OPCC sits with the Information Manager in the Force Information Management Unit. The role of the Data Protection Officer is defined in the Act and the national Data Protection Manual of Guidance and responsibilities include:

    The controller must entrust the data protection officer with at least the following tasks—

    - Informing and advising the controller, any processor engaged by the controller, and any employee of the controller who carries out processing of personal data, of that person's obligations under this Act.

    - Providing advice on the carrying out of a data protection impact assessment under section 64 and monitoring compliance with that section.

    - Co-operating with the Information Commissioner.

    - Acting as the contact point for the Information Commissioner on issues relating to processing, including in relation to the consultation mentioned in section 65, and consulting with the Commissioner, where appropriate, in relation to any other matter.

    - Monitoring compliance with policies of the controller in relation to the protection of personal data, and

    - Monitoring compliance by the controller with this Act.

Information Asset Owners

99. It is the responsibility of all staff members who have a role as an Information Asset Owner to ensure that the information asset is correctly and effectively managed in accordance with the principles of the GDPR and Data Protection Act. This includes what information is held, what is added and what is removed, how the information is moved and who has access and why.

Line Managers/Supervisors

100. It is the responsibility of all staff members who have a supervisory role to ensure that their staff operate within the terms of the GDPR and Data Protection Act 2018, and any associated OPCC/Force policies and procedural guides. This must include regular checks of work to identify training and development needs in this area and to ensure that the quality of OPCC information assets is of a high standard.

All Contractors working for or on behalf of the PCC

101. There is a personal responsibility on all persons working for or on behalf of the PCC to ensure that they comply with the law, OPCC/Force policy and/or procedural guides when undertaking their duties. All staff must comply with the GDPR and Data Protection Act regarding disclosures and exemptions with guidance contained in operating rules, conventions, policies and procedures for each system or business area.

Related Appendices

Appendix 1 - Administration and Processing of Subject Access Requests
Appendix 2 - Subject Access Request form
Appendix 3 - General Processing Rectification process
Appendix 4 - General Processing Restriction process
Appendix 5 - General Processing Erasure & Objection process

Monitoring/Review

102. Subject to any new legislation or changes in case law, which require immediate amendments, this document will be reviewed on a bi-annual basis by the Force Data Protection & FOI Manager in the Force IMU.

Who to contact about this policy

103. This policy is owned by the OPCC Corporate Administration Officer and any enquiries about this policy should be directed to John King, Corporate Administration Officer, OPCC.