

Office of the Police & Crime Commissioner

REQUEST FOR POLICE & CRIME COMMISSIONER DECISION - (N° 012 / 2018)

TITLE: Joint Data Protection Officer

Executive Summary:

The implementation of the General Data Protection Regulations places a mandatory requirement for the Office of the Police and Crime Commissioner to appoint a Data Protection Officer. The legislation does make provision for organisations to share Data Protection Officers

Recommendation:

The OPCC Executive Team are asked to:

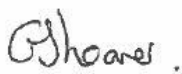
- Approve the proposal to have a Joint Data Protection Officer with Cumbria Constabulary with no associated costs levied against the OPCC; and
- Consider and comment upon the proposed role profile

Police & Crime Commissioner

I confirm that I have considered whether or not I have any personal or prejudicial in this matter and take the proposed decision in compliance with the Code of Conduct for Cumbria Police & Crime Commissioner. Any such interests are recorded below.

I hereby approve/do not approve the recommendation(s) above

~~Police & Crime Commissioner~~ / Chief Executive (delete as appropriate)



Signature:

Date:20/04/2018.....

PART 1 – NON CONFIDENTIAL FACTS AND ADVICE TO THE PCC

1. Introduction & Background

- 1.1 The implementation of the GDPR and the Directive will bring about a significant change to data protection legislation and will require organisations, which process personal data to make changes to the way in which they do so. Notwithstanding the impending departure from the European Union, the UK will still be required to adopt similar standards to the Directive and Regulation to be seen as adequate in the eyes of remaining Member States. If any country wishes to share data with EU Member States, or for it to handle EU citizens' data, they will need to be assessed as providing an adequate level of data protection.

2. Issues for Consideration

- 2.1 The proposed legislation seeks to professionalise the Data Protection Officer role and sets mandatory requirements for public authorities. The recently published Data Protection bill requires a data controller to designate a data protection officer, taking due regard of the professional qualities of the proposed officer and the proposed officer's expert knowledge of data protection law and practice and the ability to perform the specific tasks set out in the legislation.
- 2.2 Presently, the role of Data Protection Officer is undertaken on behalf of the Chief Executive, by the Governance Manager. However, the role profile for the post does not adequately reflect the responsibilities of a Data Protection Officer, as they are currently set in the draft Data Protection Bill. Please see the attached document that contains the relevant provisions from the Bill, in so far as they currently relate to this role ([Appendix 1](#)).
- 2.3 As can be seen there is provision for organisations to share a Data Controller. Having a joint Data Controller with Cumbria Constabulary has been explored and considered appropriate. A potential role profile has been developed and is attached ([Appendix 2](#)) for consideration. The predominant workload in relation to this area would be with Cumbria Constabulary, therefore it is proposed that the role would be appointed from within the Constabulary with no associated costs levied against the OPCC.
- 2.4 On 20 December 2017 the Executive Team agreed to progress the scoping of a Joint Data Protection Officer with Cumbria Constabulary. Following this a draft role profile was prepared and considered by the Executive Team on 14 March 2018 and subsequently agreed in principle.
- 2.5 Once fully agreed and appointed the name and contact details of the Joint Data Protection Officer. Work will continue to progress the practicalities of this role between the two organisations.

3. Implications

- 3.1. Financial – failure by the OPCC to comply with the new legislation could lead to financial penalties up to 20m Euros.
- 3.2. Legal - the new General Data Protection Regulations will become statute and therefore the OPCC will be required to comply with them.
- 3.3. Risk - should the OPCC fail to ensure that it processes and stores data in line with legislation it risks heavy financial penalties, adverse publicity and potential litigation.
- 3.4. HR / Equality - the new legislation has increased the rights of individuals to have their information processed fairly and where necessary removed.
- 3.5. I.T. - the OPCC website will need to ensure that it complies with the new legislation.

4. Backgrounds / supporting papers

(List any relevant business case, EIA, PID, Media Strategy and append to this form; list persons consulted during the preparation of the report)

Public Access to Information

Information in this form is subject to the Freedom of Information Act 2000 (FOIA) and other legislation. Part 1 of this form will be made available on the PCC website within 3 working days of approval. Any facts/advice/recommendations that should not be made automatically available on request should not be included in Part 1 but instead on the separate Part 2 form. Deferment is only applicable where release before that date would not compromise the implementation of the decision being approved.

Is the publication of this form to be deferred? YES / ~~NO~~

If yes, for what reason: The role profile is also to be approved by Cumbria Constabulary's Chief Officer Group, following which it will be evaluated and advertised. To publish this information prior to approval by all parties and before the process is complete may mean that incorrect information is placed within the public domain.

Until what date (if known): 25 May 2018

Is there a **Part 2** form - ~~YES~~ / NO

(If Yes, please ensure Part 2 form is completed prior to submission)

ORIGINATING OFFICER DECLARATION:

I confirm that this report has been considered by the Chief Officer Group and that relevant

financial, legal and equalities advice has been taken into account in the preparation of this report.

Signed: ...*Joanne Head*..... Date:

OFFICER APPROVAL

Chief Executive / ~~Deputy Chief Executive~~ (delete as appropriate)

I have been consulted about the proposal and confirm that financial, legal and equalities advice has been taken into account in the preparation of this report. I am satisfied that this is an appropriate request to be submitted to the Police and Crime Commissioner / Chief Executive (delete as appropriate).

Signature:

Date:

Media Strategy

The decision taken by the Police & Crime Commissioner may require a press announcement or media strategy.

Will a press release be required following the decision being considered? ~~YES~~ / NO

If yes, has a media strategy been formulated? YES / NO

Is the media strategy attached? YES / NO

What is the proposed date of the press release:

67 Designation of a data protection officer

- (1) The controller must designate a data protection officer, unless the controller is a court, or other judicial authority, acting in its judicial capacity.
- (2) When designating a data protection officer, the controller must have regard to the professional qualities of the proposed officer, in particular—
 - (a) the proposed officer's expert knowledge of data protection law and practice; and
 - (b) the ability of the proposed officer to perform the tasks mentioned in section 69.
- (3) The same person may be designated as a data protection officer by several controllers, taking account of their organisational structure and size.
- (4) The controller must publish the contact details of the data protection officer and communicate these to the Commissioner.

68 Position of data protection officer

- (1) The controller must ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.
- (2) The controller must provide the data protection officer with the necessary resources and access to personal data and processing operations to enable the data protection officer to—
 - (a) perform the tasks mentioned in section 69, and
 - (b) maintain his or her expert knowledge of data protection law and practice.
- (3) The controller—
 - (a) must ensure that the data protection officer does not receive any instructions regarding the performance of the tasks mentioned in section 69;
 - (b) must ensure that the data protection officer does not perform a task or fulfil a duty other than those mentioned in this Part where such task or duty would result in a conflict of interests;
 - (c) must not dismiss or penalise the data protection officer for performing the tasks mentioned in section 69.
- (4) A data subject may contact the data protection officer with regard to all issues relating to—
 - (a) the processing of that data subject's personal data, or
 - (b) the exercise of that data subject's rights under this Part.
- (5) The data protection officer, in the performance of this role, must report to the highest management level of the controller.

69 Tasks of data protection officer

- (1) The controller must entrust the data protection officer with at least the following tasks—

- (a) 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 Part,
 - (b) providing advice on the carrying out of a data protection impact assessment under section 62 and monitoring compliance with that section,
 - (c) co-operating with the Commissioner,
 - (d) acting as the contact point for the Commissioner on issues relating to processing, including in relation to the consultation mentioned in section 63, and consulting with the Commissioner, where appropriate, in relation to any other matter,
 - (e) monitoring compliance with policies of the controller in relation to the protection of personal data, and
 - (f) monitoring compliance by the controller with this Part.
- (2) In relation to the policies mentioned in subsection [\(1\)\(e\)](#), the data protection officer's tasks include—
- (a) assigning responsibilities under those policies,
 - (b) raising awareness of those policies,
 - (c) training staff involved in processing operations, and
 - (d) conducting audits required under those policies.
- (3) In performing the tasks set out in subsections [\(1\)](#) and [\(2\)](#), the data protection officer must have regard to the risks associated with processing operations, taking into account the nature, scope, context and purposes of processing.

**Cumbria Constabulary
HAY JOB PROFILE**

**Job Title: Force Disclosure Manager/
Data Protection Officer** **Department: People Department**

Reports To: Detective Superintendent, PSD **Location: Police Headquarters**

All employees must ensure compliance with the Cumbria Constabulary Health and Safety Policy, and all other relevant statutory Health and Safety legislation
This job profile has been written primarily for evaluation purposes and may not detail some less major duties allocated to the potholder, nor cover duties of a similar nature, commensurate with the grade, which may from time to time be reasonably required by the relevant manager.

1. JOB PURPOSE

Designated by the Chief Constable (and Police and Crime Commissioner) to act as Data Protection Officer, in accordance with the requirements contained in Article 37 of the EU General Data Protection Regulation (GDPR) and Section 69 of the Data Protection Act 2018. This is a statutory post

In brief, the post-holder will act as an independent expert on Data Protection law and practice, providing advice to the Chief Constable (and Police and Crime Commissioner) in their capacity(ies) as Data Controller of Cumbria Constabulary (and the Office of Police and Crime Commissioner for Cumbria(OPCC)),and staff, on all aspects concerning the processing, and proposed processing, of personal data.

The post-holder will also provide the strategic lead to the Force Disclosure & Vetting Section and manage the provision of a comprehensive service relating to the disclosure and management of information, vetting, information security, records management.

As a member of the People Department Senior Management Team, contribute towards the efficient running of the department.

2. PRINCIPAL ACCOUNTABILITIES

In accordance with statutory requirements, the post-holder will undertake the following tasks:

Data Protection

- 2.1** Inform and advise the Data Controller (the Chief Constable) (and Police and Crime Commissioner), any data processor engaged by the controller, and any employee of the controller who carries out processing of personal data, of that person's obligations under Data Protection legislation.
- 2.2** Provide expert advice on the carrying out of data protection impact assessments and monitor compliance with this requirement,
- 2.3** Act as the contact point for the Information Commissioner on issues relating to processing, including in relation to the consultation required by section 65 of the Act, and consulting with the Commissioner, where appropriate, in relation to any other matter,
- 2.4** Co-operate with the Information Commissioner,
- 2.5** Develop and monitor compliance with policies of the data controller in relation to the protection of personal data.

In relation to the policies mentioned above, the post-holders tasks include—

- (a) assigning responsibilities under those policies,
- (b) raising awareness of those policies,
- (c) training staff involved in processing operations, and
- (d) conducting audits required under those policies.

- 2.6 Monitor compliance by the controller with data protection legislation.
- 2.7 Act as the first point of contact for individuals whose personal data is processed, e.g. members of the public, employees etc.
- 2.8 In performing the tasks set out above, the post-holder will have regard to the risks associated with processing operations, taking into account the nature, scope, context and purposes of processing.

In addition to the specific tasks relating to data protection referred to above, the post-holder is also responsible for the following data protection related tasks;

- 2.9 Provide expert advice to the Chief Constable (and the Police and Crime Commissioner) regarding the requirement to report personal data security breaches to the Information Commissioner and make the appropriate referral to the Information Commissioner, when required to do so providing any further updates as may be required.
- 2.10 Liaise with ICT and Information Asset Owners to ensure that the requirements of data protection are incorporated into the development of systems and processes at an early stage enabling those requirements to be dealt with as business as usual.
- 2.11 Provide the strategic direction and have responsibility on behalf of the Chief Constable (and the Police and Crime Commissioner) for all matters relating to the processing of personal data under the Data Protection Act and EU GDPR.
- 2.12 Manage the processing of 'subject access requests' received by Cumbria Constabulary (and the Office of the Police and Crime Commissioner for Cumbria) ensuring responses are provided within statutory timescales and fulfil all legislative requirements.
- 2.13 Provide advice and guidance to senior managers and staff on general information disclosure related matters, ensuring that information is managed and shared in accordance with relevant legislation and that disclosure decisions are made at the appropriate level of authority.
- 2.14 Assist in the investigation of complaints of unlawful disclosure of information; research and provide information required, briefing investigating officer(s) as necessary and recommend possible remedial action.
- 2.15 Provide regular reports to the Chief Constable and the Police and Crime Commissioner in respect of the state of compliance for the organisations for which they are the Data Controller

Freedom of Information

- 2.16 On behalf of the Chief Constable, provide the strategic direction for, and manage all aspects of, Cumbria Constabulary's compliance with the Freedom of Information Act 2000 and the Environmental Information Regulations 2004, providing expert advice to officers and staff of all seniorities.
- 2.17 Act as Decision Maker to determine the applicability of exemptions which permit the lawful withholding of information and, where applicable, identifying and assessing public interest considerations. Act as an independent reviewer of complaints about such disclosures where an applicant is dissatisfied with how their request has been dealt with.
- 2.18 Manage the Cumbria Constabulary Freedom of Information Publication Scheme ensuring it is updated

with all relevant material and that information is removed, in accordance with the Freedom of Information Act, Force Policy and College of Policing Authorised Professional Practice

Other Duties

- 2.19** Manage the overall performance and welfare needs of the Disclosure & Vetting Section and, in conjunction with team leaders, be responsible for the selection, induction and facilitation of training of new members of staff. This includes the ongoing training and development of existing staff and undertaking team leader performance PDR's and 15 week reviews.
- 2.20** Provide the strategic direction for the Disclosure & Vetting Section in respect of
- Information Security and Records Management
 - Disclosure & Barring Service checks and common law police disclosures to third parties;
 - Vetting of all Constabulary personnel and prospective personnel, estate/ICT Contractors and, where appropriate, staff of partner agencies;
 - Family Court Disclosures required under the 2013 Protocol and Court Orders
 - Miscellaneous disclosure requests from insurance companies, solicitors and members of the public
- 2.21** Chair/contribute to meetings and conferences both within and outside the force area relating to these areas of business. Lead on policy and procedure implementation for all teams within the Force Disclosure & Vetting Section.
- 2.22** Act as the "Business Owner" with regards to the Primary Nominal function and Search Tool for Addresses and Names (STAN).
- 2.23** Be accountable for all service level agreements (SLAs) and memorandum of understanding (MoU) in place within the unit and put in effective measures to ensure these agreements are met. Arrange processes for quality assurance checks on functions carried out within the department.
- 2.24** Maintain the department risk register for matters appertaining to disclosure. Put measures in place to mitigate / reduce / transfer these risks.
- 2.25** Undertake any other duties commensurate with the grading of this position.

Should the following still be included??

- Implement plans to generate efficiencies and budgetary savings within the department. Take a risk based approach in developing the structure of the department. Develop options for consideration around collaboration and shared services.
- Provide the strategic direction for all matters relating to the Management of Police Information and Data Quality Standards across all business areas that manage police information. Ensure compliance with the Constabulary's Information Management Strategy (IMS).
- As a member of the People Department Senior Management Team contribute to the decision making processes within the department. Support the Head of the People Department in achieving the objectives set out in the departmental performance contract.
- Responsible for supporting and advising the Chief Information Officer in promulgating Cumbria Constabulary policies and business processes for compliance with the Management of Police Information.
- Develop solutions to enable the linking of different business areas in order to provide a consistent approach to data disclosure and to put in place a corporate charging scheme across the constabulary for the provision of such data.
- Responsible for the delegation of tasks for the improvement of Health and Safety within PSD

3. DIMENSIONS

The role of Data Protection Officer is a statutory post and the responsibilities of the post-holder must include the tasks contained within Article 39 of the EU GDPR and Section 71 of the Data Protection Act 2018.

The Data Controller (Chief Constable for Cumbria Constabulary (and Police and Crime Commissioner for the Office of Police and Crime Commissioner) is required to designate a data protection officer having regard to the professional qualities of the proposed officer and, in particular, the proposed officer's expert knowledge of data protection law and practice and the ability of the proposed officer to perform the tasks set out in legislation.

In accordance with the provisions contained within Article 37(2) of the EU GDPR and Section 69(3) of the Data Protection Act, the Chief Constable and the Police and Crime Commissioner, in their capacities as Data Controllers' for Cumbria Constabulary and the Office of the Police and Crime Commissioner for Cumbria, have agreed that the post of Force Disclosure Manager will be designated as Data Protection Officer for both organisations.

The Force Disclosure Manager will be required to provide expert advice to all officers and staff of both Cumbria Constabulary (and the OPCC) relating to data protection and will be required to have a detailed knowledge of the processing of data undertaken within the Constabulary (and within the OPCC).

The legislative changes greatly enhance the rights and freedoms of data subjects and significantly increase the monetary penalties which can be imposed by the Information Commissioner, as a result of a contravention of data protection legislation, from £500,000 to £17,000,000. The emphasises the importance of the advice the post-holder will provide, given the potential for a significant monetary penalty for contravening the legislation.

The post-holder will have first line supervisory responsibility for the Disclosure Unit Manager/legal advisor, the Vetting and Records Manager, the Records and Information Security Manager and the Senior Disclosure and Compliance Officer. The post will have second and third line management responsibility for staff within these teams (approx. 26 staff in total). The post-holder is also responsible for the budget (approximately £300,000 pa) for the externally funded Disclosure Unit.

The post-holder will also have responsibility for developing and implementing plans in place to generate efficiencies and budgetary savings within the department. This will include the restructuring of the department to drive out efficiencies and developing options for consideration around collaboration and shared services. The post holder will explore all options for cost recovery within the department in order to recoup expenditure for disclosures when appropriate, and thereby contribute to efficiency savings for the Department.

The post holder must also be aware of the potential legal and financial ramifications, which may result through the work of the Unit, by the inappropriate or inaccurate sharing of information, and the public protection risks and impact upon the reputation of the Constabulary (and the OPCC).

This person will be required to be vetted as a minimum to SC level

4. KEY FEATURES

4.1 Framework and Boundaries

When designating a data protection officer, legislation requires that the controller (eg Chief Constable) is required to have regard to the professional qualities of the proposed officer, in particular— (a) the proposed officer's expert knowledge of data protection law and practice, and (b) the ability of the proposed officer to perform the tasks mentioned in section 71.

Therefore, in order that the Chief Constable and Police and Crime Commissioner are able to designate the post-holder to the role of Data Protection Officer, the post-holder is required to have significant previous experience working in a senior data protection role within a law enforcement agency, and be able to demonstrate an expert knowledge of data protection law and practice.

Section 70(3) of the Act expressly states that instructions about the performance of the tasks referred to in Section 71, which the data protection officer is required by law to undertake, must not be given to the data protection officer. This emphasises the independence of the role and the fact that the post-holder has significant latitude to act on his/her own initiative in respect of the execution of those tasks, in accordance with his/her interpretation of the requirements of data protection legislation.

The post-holder is responsible for ensuring that up to date policies and procedures are in place, and appropriate training is available, to all officers and staff of Cumbria Constabulary and the OPCC to facilitate compliance with the EU General Data Protection Regulations and Data Protection Act 2018.

To fulfil the statutory tasks, the post-holder will provide expert advice on all issues relating to data protection. In particular, given the nature of the functions undertaken by Cumbria Constabulary, and the fact that processing of data is likely to result in a high risk to the rights and freedoms of individuals, there will be an ongoing requirement to provide advice to Information Asset Owners, project teams and ICT regarding the need to undertake data protection impact assessments.

The post-holder will also ensure the Constabulary complies with the Freedom of Information Act 2000, the Environmental Information Regulations 2004 and that ongoing activities within the Constabulary aimed at complying with the Management of Police Information (MOPI), also support compliance with data protection legislation, providing advice and support as is necessary to achieve these aims.

The post-holder must have an excellent knowledge and understanding of public protection legislation and processes and the findings and recommendations of the Bichard Inquiry.

The post-holder will be expected to write policies and procedures aimed at ensuring compliance with all areas of legislation which fall into the scope of the role, and to monitor compliance with those policies.

The post holder will perform their duties in compliance with all relevant legislation and in cognizance of relevant Home Office Circulars, protocols, manuals of guidance, information sharing agreements, service level agreements, frameworks, memoranda of understanding and codes of practice

4.2 Important Working Relationships

Internal

- Chief Officer Team, in particular the Chief Constable as the Data Controller for Cumbria Constabulary and the Deputy Chief Constable as the Senior Information Risk Owner (SIRO).
- Police and Crime Commissioner for Cumbria (as Data Controller for the OPCC) and members of the OPCC Executive Board
- Head of People Department
- Information Asset Owners
- Officers and staff of the People Department
- Legal Services
- Public Protection Units
- Employee Relations
- Marketing and Media
- ICT
- Project Teams

External

- Disclosure and Barring Service Police Liaison Manager

- DBS Standards and Compliance Unit
- Information Commissioner's Office
- NPCC Central Referral Unit
- Regional and national police data protection working groups

4.3 Major Challenges

The post was originally created as a result of civilianisation of the Chief Inspector (Disclosure) role. The requirements of the role have since evolved significantly culminating in the requirement to oversee compliance with the biggest changes to data protection legislation for a generation, across Cumbria Constabulary and the OPCC

As a consequence of the revised legislation, there is a requirement for the post-holder to oversee significant change to the way in which personal data is processed by the Constabulary and the OPCC, and to devise and embed new practices in to the 'business as usual' procedures of both organisations. This will require a culture change and as such the post-holder will be required to influence existing thinking of senior managers, in order to expedite the required changes to processes, which may well impact upon the work of other departments at a time of diminishing budgets.

There are also significant other challenges within the Disclosure & Vetting Section arising from enhanced vetting requirements contained within the Vetting Code of Practice and the limited control available over the external funds provided to the Constabulary by the Disclosure and Barring Service, in connection with the provision of safeguarding checks for employment and barring services.

The complexity and volume of demands placed on the Data Control Unit continue to increase and, as such, risk-based decisions will need to be taken as to how this workload can be managed. Increasingly difficult decisions will be required with regards to which records should be reviewed when set against a background of diminishing resources and the need to maintain and to improve data quality standards to ensure compliance with relevant legislation and guidance.

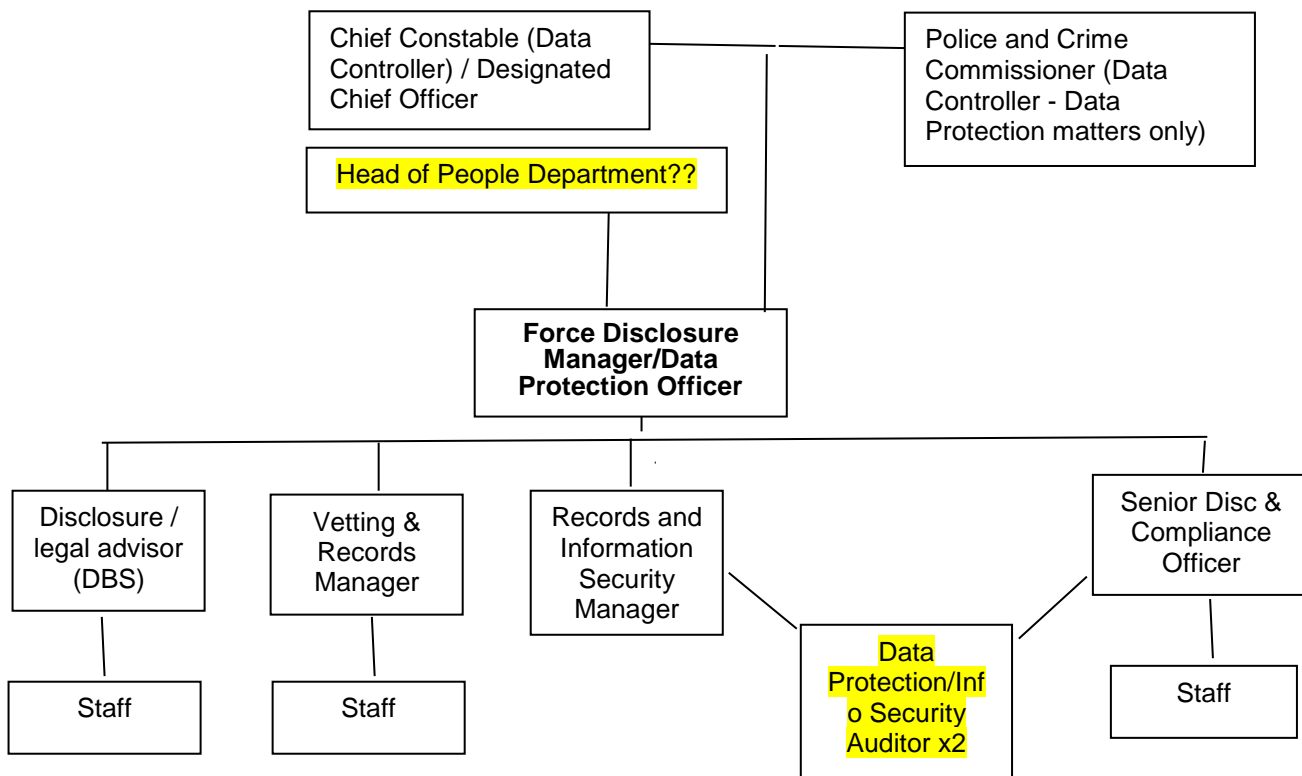
Issues over role based access, confidentiality, business owners and the security of our estate and assets have the potential to place the constabulary at risk. These are, and will continue to be addressed, through direction given at least in part, by the post-holder.

4.4 Knowledge, Skills and Experience

- Degree level or demonstrable academic competence.
- Significant supervisory experience
- Significant experience of risk assessment and risk management
- Demonstrable experience at researching and developing proposals and making strategic decisions.
- Detailed knowledge of the Code of Practice and APP Guidance on the Management of Police Information and an understanding of the content and recommendations of Bichard Report.
- ISEB/BCS Certificate in Data Protection/BCS, or equivalent
- Minimum of 5 years' experience working in a senior data protection role within a law enforcement agency
- Extensive knowledge of Freedom of Information legislation and experience gained in an FOI decision making role.
- Completion of the NPCC FOI Decision Maker course or equivalent
- Significant experience of interpreting and applying legislation, guidance and case law and proven ability to analyse and evaluate information to make informed decisions/recommendations.
- Proven effective written and verbal communication skills together with experience in policy and report writing.
- Experience of dealing with budgets
- Demonstrable experience in managing change
- Sound knowledge of the principles of information security
- Understanding of:
 - NPJA 01/2010 Police Officer Recruitment
 - National Vetting Policy and Code of Practice
 - NPCC/CAFCASS Disclosure Protocol

- Human Rights Act 1998
- Data Protection Act 2018 and EU General Data Protection Regulations
- Freedom of Information Act 2000 and Environmental Information Regulations 2004
- PNC Manual of Guidance
- Disclosure & Barring Service Quality Assurance Framework (QAF)
- ⇨ Common Law Police Disclosure Scheme
- Part V of the Police Act 1997
- Safeguarding Vulnerable Groups Act 2006 and VBS
- Cabinet Office Security Policy Framework
- Business continuity planning
- National Policing Community Security Policy
- Audit and Inspection
- Family Court Disclosure Protocol
- Information Management Strategy

5. ORGANISATION CHART



Agreed by Post Holder: _____ Date: _____

Line Manager: _____ Date: _____

Head of Department/
Division: _____ Date: _____

CUMBRIA CONSTABULARY

PERSON SPECIFICATION

JOB: Force Disclosure Manager

POST No:

LOCATION: People Department, Corporate Support, HQ

	Essential	Desirable
<p>EXPERIENCE AND KNOWLEDGE</p> <p>Skills & competencies required</p> <p>Eg Geographical knowledge of the area, familiarity with certain legislation</p>	<p>Expert knowledge of data protection law and practice, including the EU GDPR and Data Protection Act 2018.</p> <p>Minimum of 5 years experience working in a senior data protection role, preferably within a law enforcement agency</p> <p>In depth knowledge of the processing of personal data undertaken by Cumbria Constabulary and the OPCC</p> <p>Extensive knowledge of the Freedom of Information Act 2000 and experience of acting as a Decision Maker in respect of information requests</p> <p>Significant experience of risk assessment and risk management</p> <p>Demonstrable experience at researching and developing proposals and making strategic decisions</p> <p>Extensive knowledge of the Code of Practice and APP Guidance on the Management of Police Information and a sound understanding of the content and recommendations of Bichard Report.</p> <p>Experience of interpreting and applying legislation, guidance and case law and analysing and evaluating information to make decisions/recommendations.</p> <p>Proven effective written and verbal communication skills including experience in policy and report</p>	<p>Understanding and knowledge of:</p> <ul style="list-style-type: none"> • NPIA 01/2010 Police Officer Recruitment • National Vetting Policy and Vetting Code of Practice • NPCC/CAFCASS Disclosure Protocol, • Human Rights Act 1998 • PNC Manual of Guidance • DBS Quality Assurance Framework (QAF) • Common Law Police Disclosure Scheme • Part V of the Police Act 1997 • Safeguarding Vulnerable Groups Act 2006 • Vetting & Barring Scheme • ISO 27001 • Cabinet Office Security Policy Framework • Business continuity planning • National Policing Community Security Policy • Audit and Inspection • Family Court Disclosure Protocol • Information Management Strategy <p>Proficient in the use of computer applications with good knowledge of police information systems</p>

	<p>writing</p> <p>Experience of budget management</p> <p>Demonstrable experience in managing change</p>	
<p>EDUCATION AND TRAINING</p> <p>General education</p> <p>Specialist training</p>	<p>Degree level or demonstrable academic competence</p> <p>Qualification in supervisory management, or significant supervisory experience</p> <p>ISEB/BCS Certificate in Data Protection, or similar</p> <p>Completion of NPCC Freedom of Information Decision Makers training course, or equivalent</p>	
<p>Policing Professional Framework</p>	<p>Serving the public</p> <p>Leading Change</p> <p>Leading People</p> <p>Managing Performance</p> <p>Professionalism</p> <p>Decision Making</p> <p>Working with Others</p>	