CIVIL NUCLEAR CONSTABULARY

The Executive Office
Civil Nuclear Constabulary
Building F6 Culham Science Centre
Abingdon
Oxon
OX14 3DB
Tel: 03303 135400
Website: https://www.gov.uk/cnc

Email

info@ukcorruptpolice.com

26th January 2022

Dear Mr Ponting

I am writing in response to your request for information regarding the below**.** Your request has been handled under Section 1(1) of the Freedom of Information Act 2000. In accordance with Section 1(1) (a) of the Act I hereby confirm that the CNC/CNPA does hold information of the type specified.

I am writing to you under the Freedom of Information Act 2000 to request the following information from your force.

Please can you provide me with:

- **Copies of any Data Protection agreement(s) that police constables or police staff ('police employee') sign or agree when they join the force, and before they handle (or have access to) the personal data of the public, personal data acquired while in their role as police employees ('personal data').**
- **Any internal police guidance, procedures or policies for police employees that mishandle or allegedly mishandle personal data. ('data breach') that was acquired while in the role of a police employee.**
- **Please include for a data breach while on duty, off duty or after the cessation of employment, by any means.**
- **Please indicate who is responsible for investigating and/or taking appropriate action against any police employee (ex-employee) for such mishandling of personal data? Please**

include the same for on-duty, off duty or after employment cases.

- **Who is responsible for a said data breach? Again, this is for police employees on-duty, off-duty and after employment.**
- **Who is accountable for a said data breach? Again, this is for police employees on-duty, off-duty and after employment.**
- **Who is responsible for holding the police employee under any of these circumstances.**

Police staff do not sign a data protection agreement. During the induction process with their line manager handling data / records, confidentiality and reporting data breaches is covered. A checklist is given to the line manager when the new starter starts which they must go through. I have attached a copy to this letter. All new Police staff attend an induction day where they are given a presentation on GDPR by the Information Governance Team and one on security by the Security manager.

Police Officers are required to sign the following:
• Blue Lines Charter – This is borne out of the Code of Ethics and covers a number of areas. One specifically covers confidentiality and treating information correctly.
• Corporate Induction register – The students spend a whole day receiving inputs from departments within the organisation. Specific inputs cover GDPR (delivered by the Information Governance Team) and Security (delivered by the Security Manager).
• Attestation – Students are attested in the presence of a Magistrate, whereby they swear the police oath to uphold the law and treat everyone with fairness and impartiality. This attestation ties them to the law, the organisation and its policies.

The standards of professional behaviour for police officers have a specific standard entitled Confidentiality which states “Police officers treat information with respect and access or disclose it only in the proper course of police duties”. These standards are introduced to IFC’s as part of the PSD input in week 1 of the course. The Code of Ethics for policing mirrors this and applies to all working for the police, therefore include Police staff and contractors.

Please find attached Copies of the following policies:
Privacy Notice Policy
Personal Data Breach Notification Policy
Data Protection Policy Statement

The Data Protection Policy applies to all Employees and interested parties of the Constabulary such as outsourced suppliers. Any breach of the GDPR, the data protection legislation or this Policy will be dealt with under the Constabulary's disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities".

The DPO collates reports of data breaches and investigates in the first instance before referring to PSD and/or HR if required (as well as assessing whether a breach requires reporting to the ICO)?

Any serious data breach, if deemed to be a criminal act, would be dealt with by local police and any subsequent conviction would be dealt with by PSD (officers) as a breach of professional standards or by HR (staff) under relevant procedures. Any data breach which would not reach the criminal threshold/definition may constitute a breach of professional standards (police officers) under the above 'confidentiality' or any breach of our internal policies would also be dealt with under 'Orders and Instructions' The police standards apply equally when on or off duty. Police staff breaches of policy would be dealt with under the relevant Police staff misconduct policy.

Criminal breaches can be reported or investigated after the employee has left the organisation, and in the case of police officers, they can be investigated for misconduct if the allegation was made before they resigned or in cases reported after they left, within 12 months of the leaving date.

The Civil Nuclear Constabulary is a specialist armed police service dedicated to the civil nuclear industry, with Operational Policing Units based at 10 civil nuclear sites in England and Scotland and over 1600 police officers and staff. The Constabulary headquarters is at Culham in Oxfordshire. The civil nuclear industry forms part of the UK's critical national infrastructure and the role of the Constabulary contribute to the overall framework of national security.

The purpose of the Constabulary is to protect licensed civil nuclear sites and to safeguard nuclear material in transit. The Constabulary works in partnership with the appropriate Home Office Police Force or Police Scotland at each site. Policing services required at each site are greed with nuclear operators in accordance with the Nuclear Industries Security Regulations 2003 and ratified by the UK regulator, the Office for Nuclear Regulation (ONR). Armed policing services are required at most

civil nuclear sites in the United Kingdom. The majority of officers in the Constabulary are Authorised Firearms Officers.

The Constabulary is recognised by the National Police Chiefs' Council (NPCC) and the Association of Chief Police Officers in Scotland (ACPOS). Through the National Coordinated Policing Protocol, the Constabulary has established memorandums of understanding with the local police forces at all 10 Operational Policing Units. Mutual support and assistance enable the Constabulary to maintain focus on its core role.

We take our responsibilities under the Freedom of Information Act seriously but, if you feel your request has not been properly handled or you are otherwise dissatisfied with the outcome of your request, you have the right to complain. We will investigate the matter and endeavour to reply within 3 – 6 weeks. You should write in the first instance to:

Kristina Keefe
Disclosures Officer
CNC
Culham Science Centre
Abingdon
Oxfordshire
OX14 3DB

E-mail: FOI@cnc.pnn.police.uk

If you are still dissatisfied following our internal review, you have the right, under section 50 of the Act, to complain directly to the Information Commissioner. Before considering your complaint, the Information Commissioner would normally expect you to have exhausted the complaints procedures provided by the CNPA.

The Information Commissioner can be contacted at:

FOI Compliance Team (complaints)
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

If you require any further assistance in connection with this request please contact us at our address below:

Kristina Keefe
Disclosures Officer
CNC
Culham Science Centre
Abingdon
Oxfordshire
OX14 3DB
E-mail: FOI@cnc.pnn.police.uk

Yours sincerely
Kristina Keefe
Disclosures Officer

INDUCTION CHECKLIST

WELCOME to the Civil Nuclear Constabulary …..

This document and checklist are to be used by you and your manager or nominated person to ensure that you receive all relevant and appropriate information for your new role. It will ensure that all aspects of induction are covered in a timely and effective manner.

This document represents a broad spectrum of good practices and advice but is not intended to be exhaustive. This document forms part of the induction process and must be satisfactorily completed within 6 months of joining the Civil Nuclear Constabulary (CNC).

This checklist should be:

· Constantly reviewed during and at the end of the 6-month period
· Checked to ensure that all areas have been covered
· Signed off by you
· Signed off by your line manager
· Filed on your individual HR Personal File (copy to be retained by you)

Annual Performance and Career Development (PCD) objectives will be set for Police Staff by their manager and will relate to CNC targets and will assist individuals to develop into their new role. The job description and behavioural role profile will also be explained. Managers may also set up job chats to help individuals during and after the induction period.

As each item is discussed it will be dated by the person providing the information, and/or by yourself, once you feel the information has been adequately covered. Not all items are relevant to all employees (mark these with N/A) and space has been allocated for items specific to your role. If you feel that any area has been missed, and you require further information, please bring it to the attention of the person completing the induction with you.

Over the first few weeks your manager will:
· Ensure you undertake the Security Induction and the Health and Safety Induction
· Give you a variety of tasks to do related to your job role in the department/Unit
· Arrange for you to meet new people
· Supply relevant information for you to read
· Arrange shadow working if appropriate

CHECKLIST

SETTLING IN AND FINDING YOUR WAY

ITEM	DATE COMPLETED
Desk/Office Area/Department	
Tour of place of work. Identify areas of key Departments	
The CNC core values	
Fire Exits	
Kitchen area	
Break/Lunch/Meal arrangements	
Toilets	
Stationery	
Photocopier/Fax	
Helpdesks i.e. DXC, MFSS, IT	
Parking facilities	
Post delivery/collection times	
Issue of security badges	
Notice Boards	
Introduction to team members	
Introduction to other key contacts	
Introduction to immediate contacts as a requirement of role	
Other Sites within CNC	
Demonstration of SKYPE:	
- Answering, taking messages, diverting calls, voicemail	
- Private calls	
- Phone directory	
Mobile phones (if applicable)	
Hours of Work:	
Normal hours of work	
Opening hours/accessibility of building/codes as appropriate	
Flexible working/working from home/flexi time	
Unsocial hours	
Overtime	
Break times	
Working time regulations	
Covering for colleagues	
IT, Email System & Internet:	
Crown DMS – Book On/Book Off (BOBO)	
Private use of	
Demonstrate intranet	
User guides	
Provide email address	
Add ‘Signature’	
Security requirements – no memory sticks/disks	
Oracle	
QSET (if appropriate)	
VERTO (if appropriate)	
Other Systems as appropriate (Chronicle, etc.)	

ADMINISTRATION

ITEM	DATE COMPLETED
Pay:	
Your pay is paid directly into your bank	
Pay dates – last working day of month (except Christmas)	
P45/38/46 – have you sent this to CNC Payroll	
P46 available if you don’t have a P45	

Expenses:	**DATE COMPLETED**
Claim form (Oracle I-Expenses)	
How to complete the e-form	
Mileage and rates	
Annual Leave:	
Booking through Crown DMS	
Annual leave year runs from April to March	
Carry over allowance	
Who approves	
Notice period for requesting	
Sickness:	
Reporting procedure	
Recording of sickness on Crown DMS	
UKAEA Combined Pension Scheme (CPS):	
Contacts/Equiniti Pensions website	
Transfer of pension from previous employer - if applicable	
Misc:	
Meeting room on line booking procedure	
Purchase orders using Oracle Procurement	
Finance information as appropriate	
How to address Police Staff & Officers	
Staff Associations - Prospect/Federation/Superintendents Association	
Use of gyms if appropriate (induction required)	
Welfare fund and lottery	
Occupational Health and Wellbeing	
Newsletters, articles of interest, etc	

SECURITY, PROFESSIONAL STANDARDS AND DATA PROTECTION

ITEM	**DATE COMPLETED**
Issue of:	
Photo ID Badge – complete form	
Appointment for photo	
Any security procedures appropriate to the specific role	
Professional Standards role	
Identify location of lockers (if applicable)	
Security Induction course booked:	
Information Security:	
Passwords	
Confidentiality	
Handling Data/Records - Data Protection	
Breach, near miss and concerns reporting	
Freedom of Information and Subject Access Requests	

HEALTH AND SAFETY

ITEM	**DATE COMPLETED**
Fire Procedures:	
Fire alarms and evacuation procedures	
Local fire alarm test day	
Fire assembly point	
Name of Fire Warden	
Fire Exits/extinguishers	
Occupational Health:	
VDU Screening	
Frequency of medicals (if applicable)	
Drugs & Alcohol Policy	
Emergency contact information	
First Aiders/First Aid room/First Aid box	
Accident Reporting:	**DATE COMPLETED**

Where to find the incident report forms	
Explain the reporting procedure	
No smoking sites	
Health & Safety:	
Local Health and Safety arrangements	
Health and Safety responsibilities and representatives	
Local Risk Assessments	

JOB SPECIFIC ITEMS

ITEM	**DATE COMPLETED**
Basics of the role	
Job Description/Person Specification	
Reporting procedure/structure	
Role Profile	
Departmental structure	
CNC structure	
Standards and expectations	
Probation period (6 months) and 12 week review date:	
Performance & Career Development Objectives/Review	
Date booked for review of progress and objectives at 6 months	
Development needs	
Filing systems/paper and electronic	
Standard letter/memo formats	
Team communication	
Administration support (if applicable)	
Others:	

LEARNING AND DEVELOPMENT

ITEM	**DATE COMPLETED**
Crown DMS training through NCALT	
Oracle I-Support system and knowledge articles	
NCALT - overview	
Centre for Learning & Development - F7 Culham	
Procedure for booking courses	
E-learning	
Agreed statutory and mandatory training requirements for role and requirement to complete these within the first week of employment	
Further Learning and Development to be considered as part of the Performance Development review process	

SIX MONTHS AFTER APPOINTMENT

Check that all the areas in the document have been covered

- Ensure probationary period has been reviewed and feedback returned to HR.
- Ensure a Performance and Career Development Review meeting has been arranged.
- Sign off the document, indicating that you have covered all areas.
- Take a copy of this completed document and retain for your personal records. Pass original document to HR.

NEW EMPLOYEE

I have completed the Local Induction as outlined in this document, in conjunction with my line manager. I agree that a copy of this document will be kept on my personnel file
Signed: Date:
Name:

LINE MANAGER

I confirm you have completed your induction into the CNC. I also confirm that we have arranged a 12 week probation review and a 6 monthly Performance and Career Development review meeting to take place to appraise the last 6 months and to set your future objectives
Signed: Date:
Name:

PLEASE RETAIN A COPY OF THE COMPLETED FORM AND SEND THE ORIGINAL TO HR

Data Protection Policy Statement

Policy, scope and objectives

The Civil Nuclear Constabulary (CNC) is committed to compliance with all relevant UK and EU laws in respect of personal data, and to protecting the rights and freedoms of individuals whose information the Constabulary collects in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. To that end, the CNC, on behalf of the CNPA, has developed, implemented, maintains and continuously improves an Information Governance Strategy and Framework for the Constabulary.

Scope

The scope of the Information Governance Strategy - taking into account organisational structure, management responsibility, jurisdiction and geography - includes the whole of the CNC and the CNPA.

Objectives of the Information Governance Strategy (IGS)

CNC's objectives for the IGS are that it should enable the Constabulary to meet its own requirements for the management of all information assets, including personal information; that it should support organisational objectives and obligations; that it should impose controls in line with CNC's acceptable level of risk; that it should ensure that the Constabulary meets applicable statutory, regulatory, contractual and/or professional duties; and that it should protect the interests of individuals and other key stakeholders.

The Constabulary is committed to complying with data protection legislation and good practice including:

- **Lawfulness, Fairness and Transparency**: processing personal information only where this is strictly necessary for legitimate organisational purposes and providing clear information to individuals about how their personal information will be used and by whom; processing personal information fairly and lawfully
- **Purpose Limitation**: only processing relevant and adequate personal information for the identified purpose;
- **Data Minimisation**: collecting only the minimum personal information required for the purpose and not processing excessive personal information;
- **Accuracy**: keeping personal information accurate and, where necessary, up to date;

- **Storage Limitation**: retaining personal information only for as long as is necessary for legal or regulatory reasons or, for legitimate organisational purposes;
- **Integrity and Confidentiality**: keeping all personal information secure;
- **Accountability, Roles and Responsibilities:** the identification of employees with specific responsibility and accountability for the management of information and personal data.
- **Skills and Training:** the training of all staff in Data Protection
- **Documented Process and Procedure** maintaining an inventory of the categories of personal information processed by the Constabulary, developing and implementing the Information Governance Framework to ensure that the necessary Policies, Processes and Working Instructions for every Information Asset are in place
- **Independent Audit and monitoring**
- **Data Subjects Rights:** respecting individuals' rights in relation to their personal information, including their right of subject access.

Notification

The Constabulary has notified the Information Commissioner that it is a data controller and that it processes certain information about data subjects. The Constabulary has identified all the personal data that it processes and this is contained in the Scope of Information Management Systems, the Data Flow Maps and the Data Registers.

A copy of the ICO notification details is retained by the Data Protection Officer and the notification is renewed annually on 22 February.

The Data Protection Officer is responsible, each year, for reviewing the details of notification, in the light of any changes to The Constabulary's activities (as determined by changes to the Data Registers and the management review) and to any additional requirements identified by means of data protection impact assessments.

The policy applies to all Employees and interested parties of the Constabulary such as outsourced suppliers. Any breach of the GDPR, the data protection legislation or this Policy will be dealt with under the Constabulary's disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

Partners and any third parties working with or for the Constabulary, and who have or may have access to personal information, will be expected to have read, understood and to comply with this policy. No third party may access personal data held by the Constabulary without having first entered into a data confidentiality agreement which imposes on the third-party obligations no less onerous than those to which the Constabulary is committed, and which gives the Constabulary the right to audit compliance with the agreement.

Background to the General Data Protection Regulation ('GDPR')

The GDPR replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of living individuals, and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

Definitions used by the organisation (drawn from the GDPR)

Personal data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law. The Data Controller for the Constabulary is the Chief Constable.

Data subject – any living individual who is the subject of personal data held by an organisation.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse, or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Personal data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to

report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject. All breaches and near misses are reported, investigation and recorded.

Data subject consent - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

Responsibilities under the General Data Protection Regulation

The Chief Constable of the CNC is a data controller and may be in limited circumstances a data processor under the GDPR.

The Executive of the Civil Nuclear Constabulary (CNC), the Board members of the Civil Nuclear Police Authority (CNPA) and all those in managerial or supervisory roles throughout the Constabulary are responsible for developing and encouraging good information handling practices within the organisation;

The Data Protection Officer is accountable to the CNPA Board and to the Executive of the CNC for the management of personal information within the Constabulary and for ensuring that compliance with data protection legislation and good practice can be demonstrated.

A Data Protection Officer whom the Executive considers to be suitably qualified and experienced, has been appointed to take responsibility for compliance with this policy on a day-to-day basis and, in particular, has direct responsibility for ensuring that the Constabulary complies with the data protection legislation, in respect of data processing that takes place within their area of responsibility.

The Data Protection Officer, together with the Disclosures Officer, has specific responsibilities in respect of procedures such as Subject Access Requests, and are the first point of call for Employees/Staff seeking clarification on any aspect of data protection compliance. They can be contacted by emailing:
Data.protection.officer@cnc.pnn.police.uk
Subject.access.request@cnc.pnn.police.uk

Compliance with data protection legislation is the responsibility of all members of the Constabulary, and the Constabulary's Training Policy sets out specific training and awareness requirements in relation to specific roles and to members of The Constabulary generally.

Members of the Constabulary, all employees, Officers and Staff are responsible for ensuring that any personal data supplied by them, and that is about them, to the Constabulary is accurate and up-to-date.

Risk Assessment

The Constabulary has to be aware of any risks associated with the processing of particular types of personal information and has a process for assessing the level of risk to individuals associated with the processing of their personal information. Assessments will also be carried out in relation to processing undertaken by other organisations on behalf of The Constabulary, which shall manage any risks identified by the risk assessment in order to reduce the likelihood of a non-conformance with this policy.

Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the “rights and freedoms” of natural persons, the Constabulary shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a Data Protection Impact Assessment or DPIA)

A single assessment may address a set of similar processing operations that present similar high risks.

Where, as a result of a Data Protection Impact Assessment, it is clear that the Constabulary is about to commence processing of personal information that could cause damage and/or distress to the data subjects, the decision as to whether or not the Constabulary may proceed must be escalated for review to the Data Protection Officer. The Data Protection Officer shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the Information Commissioners Office (ICO).

Appropriate controls will be selected from ISO27001 and applied to reduce the level of risk associated with processing individual data to an acceptable level, by reference to CNC’s documented risk acceptance criteria and the requirements of the GDPR.

Data protection principles

All processing of personal data must be done in accordance with the following data protection principles of the Regulation, and The Constabulary’s policies and procedures are designed to ensure compliance with them.

1. Personal data must be processed lawfully, fairly and transparently

The GDPR introduces the requirement for transparency and requires the data controller to have in place transparent and easily accessible policies relating to the processing of personal data and the exercise of individuals’ rights and freedoms. Information must be communicated to the data subject in an intelligible form using clear and plain language.

The specific information that must be provided to the data subject must as a minimum include:

- the identity and the contact details of the controller and, if any, of the controller's representative;
- the contact details of the Data Protection Officer;
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- the period for which the personal data will be stored;
- the existence of the rights to request access, rectification, erasure or to object to the processing;
- the categories of personal data concerned;
- the recipients or categories of recipients of the personal data, where applicable;
- where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;
- any further information necessary to guarantee fair processing.

2. **Personal data can only be collected for specified, explicit and legitimate purposes.**

Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the Information Commissioner as part of The Constabulary's GDPR registration.

3. **Personal data must be adequate, relevant and limited to what is necessary for processing.**

The Data Protection Officer is responsible for ensuring that information, which is not strictly necessary for the purpose for which it is obtained, is not collected.

All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must be approved by the Data Protection Officer.

The Data Protection Officer will ensure that, on an annual basis all data collection methods are reviewed by internal audit/and by external experts to ensure that collected data continues to be adequate, relevant and not excessive.

If data is given or obtained that is excessive or not specifically required by The Constabulary's documented procedures, the Data Protection Officer is responsible for ensuring that it is securely deleted or destroyed in line with policy.

4. **Personal data must be accurate and kept up to date.**

Data that is kept for a long time must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

The Head of HR is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

It is also the responsibility of individuals to ensure that data held by The Constabulary and by Third Party Suppliers on its behalf is accurate and up to date where the data is provided directly by the individual to the Third-Party Supplier via secure web portal. Completion of an appropriate registration or application form or the submission of data via on online portal will be taken as an indication that the data contained therein is accurate at the date of submission.

Employees should notify The Constabulary and any relevant Third-Party Suppliers directly of any changes in circumstance to enable personal records to be updated accordingly. Instructions for updating records are available on the intranet. It is the responsibility of The Constabulary as Data Controller, and the Multi Force Shared Service (MFSS) as Data Processor, to ensure that any notification regarding change of circumstances is noted and acted upon.

The Data Protection Officer is responsible for ensuring that appropriate additional steps are taken to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

On at least an annual basis, the Data Protection Officer will review all the personal data maintained by The Constabulary, by reference to the Data Registers, and will identify any data that is no longer required in the context of the registered purpose. The DPO will arrange to have that data securely deleted/destroyed in line with policy.

The Data Protection Officer is responsible for making appropriate arrangements - where third party organisations may have been passed inaccurate or out-of-date personal information - for informing them that the information is inaccurate and/or out-of-date and is not to be used to inform decisions about the individuals concerned, and for passing any correction to the personal information to the third party where this is required.

5. Personal data must be kept in a form such that the data subject can be identified only for as long as is necessary for processing.

Where personal data is retained beyond the processing date, it will be minimized, encrypted and/or pseudonymized as appropriate in order to protect the identity of the data subject in the event of a data breach, and a record made of the justification for retaining the data.

Personal data will be retained in line with the retention of records procedure and, once its retention date is passed, it must be securely destroyed as set out in the procedure.

The Data Protection Officer must specifically approve any data retention that exceeds the retention periods defined in the Retention of Records Procedure and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be written.

6. Personal data must be processed in a manner that ensures its security

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed. The Constabulary's compliance with this principle is contained in its Information Security Management System (ISMS), which has been developed in line with ISO/IEC 27001:2013 and the information security policy.

Security controls will be subject to audit and review.

7. Personal data shall not be transferred to a country or territory outside the European Union unless that country or territory ensures an adequate level of protection for the 'rights and freedoms' of data subjects in relation to the processing of personal data.

The transfer of personal data outside of the EU is prohibited unless one or more of the specified safeguards or exceptions apply.

Safeguards

An assessment of the adequacy by the data controller taking into account the following factors:

- the nature of the information being transferred;
- the country or territory of the origin, and final destination, of the information;
- how the information will be used and for how long;
- the laws and practices of the country of the transferee, including relevant codes of practice and international obligations; and
- the security measures that are to be taken as regards the data in the overseas location. (This is a UK-specific option.)

Model contract clauses

The Constabulary may adopt approved model contract clauses for the transfer of data outside of the EU. If The Constabulary adopts the model contract clauses approved by the relevant Supervisory Authority there is an automatic recognition of adequacy.

Exceptions

In the absence of an adequacy decision, a transfer of personal data to a third country, or an international organisation, shall take place only on one of the following conditions:

- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims;
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
- the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case.
- A list of countries that satisfy the adequacy requirements of the Commission are published in the *Official Journal of the European Union.*

Accountability

The GDPR introduces the principle of accountability which states that the controller is not only responsible for ensuring compliance but for demonstrating that each processing operation complies with the requirements of the GDPR.
Specifically, controllers are required to maintain necessary documentation of all processing operations, implement appropriate security measures, perform DPIAs (Data Protection Impact Assessments), comply with requirements for prior notifications, or approval from supervisory authorities and appoint a Data Protection Officer if required.

Potential fines for non-compliance

The maximum fine for non-compliance is 20 million Euros (or equivalent in sterling) or 4% of the total annual worldwide turnover in the preceding financial year, whichever is higher.

In practice, the higher maximum amount can apply to any failure to comply with any of the data protection principles, but where there is an infringement of the administrative requirements of the legislation – such as failure to notify the ICO of a reportable data breach - the standard maximum amount will apply, which is 10

million Euros (or equivalent in sterling) or 2% of the total annual worldwide turnover in the preceding financial year, whichever is higher.

Data subjects' rights

The GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Data subjects have these rights both regarding data processing, and the data that is recorded about them. Data Subjects wishing to exercise any of the above rights may do so by making a request to the Data protection Officer at data.protection.officer@cnc.pnn.police.uk

Data subjects also have the right to sue for compensation if they suffer damage as a result of a contravention of the GDPR and Data Protection Act 2018 and are able to contact the Information Commissioners Office direct to complain, to report a data breach, or to ask them to access whether any provision of the legislation has been breached.
.

Complaints

Data Subjects who wish to complain to The Constabulary about how their personal information has been processed may lodge their complaint directly with the Data Protection Officer by emailing data.protection.officer@cnc.pnn.police.uk or by telephoning 0330 313 5633.

Data subjects may also complain directly to the ICO https://ico.org.uk/make-a-complaint

Where data subjects wish to complain about how their complaint has been handled, or appeal against any decision made following a complaint, they may lodge a further complaint to the Data Protection Officer.

Consent

The Constabulary understands 'consent' to mean that it has been explicitly and freely given, and is a specific, informed and unambiguous indication of the data subject's wishes. This means that he or she - by statement, or by a clear affirmative

action - signifies agreement to the processing of personal data relating to him or her. The consent of the data subject can be withdrawn at any time.

The Constabulary further understands ‘consent’ to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

There must be some active communication between the parties which demonstrates active consent. Consent cannot be inferred from non-response to a communication. For sensitive data, explicit written consent must be obtained unless an alternative legitimate basis for processing exists.

In most instances the processing of personal and sensitive data by the Constabulary does not rely upon consent, but on one of the other lawful basis for processing. Where consent is relied upon The Constabulary uses standard consent documents.

Security of data

All Employees, Staff and Officers, are responsible for ensuring that any personal data which The Constabulary holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by The Constabulary to receive that information and has entered into a confidentiality agreement.

All personal data should be accessible only to those who need to use it, and access may only be granted in line with the Access Control Policy. Judgment must be based upon the sensitivity and value of the information in question, but personal data must be kept:

- in a lockable room with controlled access; and/or
- in a locked drawer or filing cabinet; and/or
- if computerised, password protected in line with corporate requirements in the Access Control Policy; and/or
- with prior authorization of the Security department, stored on (removable) computer media which are encrypted in line with the Secure Destruction of Storage Media Policy.

Care must be taken to ensure that PC screens and terminals are not visible except to authorised Employees/Staff of The Constabulary. All Employees are required to enter into an Acceptable Use Agreement before they are given access to organisational information of any sort.

Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit [written] authorisation. As soon as manual records are no longer required for day-to-day client support, they must be removed from secure archiving in line with procedure.

Personal data may only be deleted or disposed of in line with the Data Retention Procedure. Manual records that have reached their retention date are to be shredded

and disposed of as ‘confidential waste’. Hard drives of redundant PCs are to be removed and immediately destroyed as required by policy before disposal. Emails required to be retained should be stored and the original deleted from Outlook.

Processing of personal data ‘off-site’ presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised to process data off-site.

Rights of access to data

Data subjects have the right to access any personal data (i.e. data about them) which is held The Constabulary in electronic format and manual records which form part of a relevant filing system. This includes the right to inspect confidential personal references received by The Constabulary, and information obtained from third-party organisations about that person.

Subject Access Requests are dealt with by the Disclosures Officer as described in the Subject Access Request Procedure and by contacting Subject.access.request@cnc.pnn.police.uk

Disclosure of data

The Constabulary must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All Employees, Staff and Officers, should exercise caution when asked to disclose personal data held on another individual to a third party and will be required to attend specific training that enables them to deal effectively with any such risk. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of The Constabulary’s business.

The GDPR permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:

- to safeguard national security;
- prevention or detection of crime including the apprehension or prosecution of offenders;
- assessment or collection of tax duty;
- discharge of regulatory functions (includes health, safety and welfare of persons at work);
- to prevent serious harm to a third party;
- to protect the vital interests of the individual (this refers to life and death situations).

All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Data Protection Officer.

Retention and disposal of data

Personal data may not be retained for longer than it is required. Once a member of staff has left The Constabulary, it may not be necessary to retain all the information held on them. Some data will be kept for longer periods than others. The Constabulary's data retention and data disposal procedure will apply in all cases.

Disposal of records

Personal data must be disposed of in a way that protects the "rights and freedoms" of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion) and in line with the secure disposal procedure.

Document Owner and Approval

The Data Protection Officer is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above and as a minimum once per annum.

A current version of this document is available to all members of staff on the corporate intranet.

Change History Record

Issue	Description of Change	Approval	Date of Issue
1	Initial issue		25 May 2018
2	Amended in line with audit recommendations		14 November 2018
3	Amended to replace PIMS with IG Framework		12 September 2019
4	Reviewed following audit		28 Feb 2020
	Reviewed		22 Jan 2021

Personal Data Breach Notification Policy

Scope

This policy applies in the event of a personal data breach under Article 33 *Notification of a personal data breach to the supervisory authority,* and Article 34 *Communication of a personal data breach to the data subject* of the GDPR.

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

The purpose of this policy is to ensure that:

- Data breach events are detected, reported, categorised and monitored consistently.
- Incidents are assessed and responded to appropriately.
- Action is taken to reduce the impact of disclosure
- Mitigation improvements are made is put in place to prevent recurrence
- Serious breaches can be reported to the Information Commissioner
- Lessons learnt are communicated to the organisation as appropriate and can work to prevent future incidents

Responsibility

All employees, contractors or temporary Staff and third-party users and the Constabulary are required to be aware of, and to follow this procedure in the event of a personal data breach. A failure to report a data breach in accordance with this Policy will be treated as a disciplinary matter.

Procedure- Internal handling of Personal Data Breaches

Where there has been a suspected data breach, near miss or data concern the following process will be followed;

- A Breach of Security/Near Miss or Concern form will be completed and provided to the Data Protection Officer (DPO) via vetting as soon as possible after becoming aware of the potential breach, providing as much detail as possible at that time.
- The DPO will make an initial assessment of the severity of the breach.
- If there is a likelihood that the breach is ongoing the DPO will consult with the relevant departments to ensure that the breach is stopped or contained as soon as possible.
- The DPO may contact the individual or department reporting the breach for further information.
- The DPO will consider whether a notification is required under sections 3 and 4 of the policy and will consult with necessary departments.
- Where it is determined that the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms and where the DPO has decided to notify the ICO, the DPO will also notify the BEIS data protection team at dataprotection@beis.gov.uk
- The outcome of the breach will be uploaded to the Security Breach spreadsheet held by the Security department. The DPO maintains a Data Breach Register in addition.

Procedure – Breach Notification Data Controller to Supervisory Authority

The DPO shall assess whether the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach.

In assessing the extent of damage or potential damage caused consideration will be given to the volume, sensitivity and exposure of the personal data.

In assessing whether the breach is likely to result a risk to the rights and freedom of the data subjects the Constabulary shall also consider whether, if not addressed, the breach would result in physical, material or non-material damage to the data subjects or others such as loss of control over their personal data or limitation of their rights discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data

protected by professional secrecy or any other significant economic or social disadvantage to the individuals concerned.

If a risk to the aforementioned is likely the DPO shall report any personal data breach to the supervisory authority without undue delay, and where feasible not later than 72 hours. Where data breach notification to the supervisory authority is not made within 72 hours, it shall be accompanied by the reasons for the delay.

The data controller shall provide the following information to the supervisory authority, which shall be recorded on the Internal Data Breach Register:

- A description of the nature of the breach
- The categories of personal data affected
- Approximate number of data subjects affected
- Approximate number of personal data records affected
- Name and contact details of the Data Protection Officer
- Likely consequences of the breach
- Any measures that have been or will be taken to address the breach, including mitigation
- The information relating to the data breach, which may be provided in phases.

The Data Protection Officer notifies their contact within the Information Commissioners Office, which is recorded the Internal Breach Register.

Notification is made by completion of the online ICO breach report form, by phone call, or by email.

Confirmation of receipt of this information is made by email.

The DPO will then notify the data protection team at BEIS.

Procedure – Breach Notification Data Controller to Data Subject

Where the personal data breach is likely to result in high risk to the rights and freedoms of the data subject the Constabulary shall notify the affected data subjects without undue delay, in accordance with the Data Protection Officer recommendations.

The notification to the data subject shall describe in clear and plain language the nature of the breach including the information specified 4.4 above.

Appropriate measures have been taken to render the personal data unusable to any person who is not authorised to access it, such as encryption.

The controller has taken subsequent measure to ensure that the rights and freedoms of the data subjects are no longer likely to materialise.

It would require a disproportionate amount of effort. In such a scenario there shall be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

The supervisory authority may where it considers the likelihood of a personal data breach resulting in high risk require the data controller to communicate the personal data breach to the data subject.

Document Control

The Data Protection Officer is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the GDPR and as a minimum once per annum.

A current version of this document is available to members of staff on the corporate intranet.

Change History Record

Issue	Description of Change	Approval	Date of Issue
1	Initial issue		May 2018
2	Amended to reflect BEIS reporting requirements		7/8/18
3	Reviewed following audit		28/02/2020
	Reviewed	DPO	22/01/2021

Privacy Notice Policy

Scope

All processing of information about data subjects within or by the Constabulary is within the scope of this procedure.

Responsibilities

The Data Protection Officer is responsible for ensuring that the Privacy Notices are correct and that mechanisms exist for making all data subjects aware of the contents of these notices prior to the Constabulary commencing collection of their data.
All staff that may need to collect personal data are required to adhere to this policy.

Definition of a Privacy Notice

Privacy Notices (sometimes referred to as Fair Processing Notices), set out the information you need to provide to individuals from whom you collect or are intending to collect personal data.

A Privacy Notice should inform the data subjects who is collecting their data, the purpose of collecting the data, who it may be shared with and transferred to and how the Constabulary will safeguard the data. The data subjects should also be informed via the Privacy Notice of their rights, including their right to complain to the ICO.

Privacy Notices should be provided to data subjects when the Constabulary is first collecting personal data or where it intends to process existing personal data held for a new purpose. The general Privacy Notice is also made available to all employees on the corporate intranet.

Procedure

Those responsible for processing personal data may only do so where this activity has been authorised by the Data Protection Officer.

In particular, data subjects must be informed, prior to the collection of data, of the following information:

- the identity and contact details of the CNC's Data Protection Officer;
- the lawful basis for processing
- the legitimate interests of the processing;
- the categories of personal data obtained;
- the recipients or categories of recipients of the personal data;
- the right to data portability;
- the right to object to the processing of their personal data in certain circumstances;
- the data subject's rights related to automated decision making including profiling;
- details of whether individuals are under a statutory or contractual obligation to provide the personal data;
- the purposes for which personal information will be processed;
- how long the personal data will be stored, or the criteria under which it is stored;
- a description of how (if at all) this information will be disclosed to third parties;
- information about the individual's rights relating to their personal data, including the right of access to personal information, right to withdraw consent, right to rectify personal data, right to have personal data erased, right to strict processing, the right to lodge a complaint with the Information Commissioners Office;
- whether personal information is transferred outside the European Union, and whether the destination has been the subject of an adequacy decision or a reference to the safeguards in place;
- details of any automated processing, such as profiling, that will be performed on the personal data supplied;
- whether the personal data must be supplied to fulfil or enter into a contract, as well as whether there are any possible consequences of failing to provide personal data;
- any other information that would make the processing fair.

All such information provided to data subjects is in clear, plain language.

This information is contained in the Privacy Notice issued to all data subjects before the Constabulary processes their data.

The Data Protection Officer shall incorporate procedures that indicate, where processing has been based upon consent and the consent is withdrawn, that consent has been withdrawn and that processing based on that consent will cease.

When determining the basis on which the processing is taking place it should be remembered that consent will not normally be an appropriate ground between an employer and an employee as the parties are not normally deemed to be on an equal footing and therefore the consent cannot be said to be freely given.

The Data Protection Officer is responsible for monitoring all requests for removal of withdrawals of consent and maintains a register of all such requests and ensures that all removals are completed within 24 hours.

Where sensitive personal information is being collected for a particular purpose(s), the Data Protection Officer shall be consulted to ensure that the Privacy Notice explicitly states the purpose(s) for which sensitive personal information is or might be used.

Where data processing relates to a child (16 years or younger) the Data Protection Officer shall ensure The Constabulary has obtained and recorded consent provided by the holder of parental responsibility over the child.

The Data Protection Officer is responsible for ensuring that all new data collection methods are reviewed and signed off to ensure that such methods can be demonstrated as compliant with data protection legislation and good practice.

Privacy Notices

The Data Protection Officer is responsible for maintaining a register of Privacy Notices which identifies for each Privacy Notice (PN) the version number, the issue and withdrawal dates, the locations used and, by reference to the data collection purposes, the purposes for which personal data is collected.

Specified Purposes

Personal data may only be processed for the purpose for which it was originally collected. All requests for changes to the use of personal data must be put in writing using plain language that is clear and concise which sets out the original purpose, the proposed new or additional purpose and the reason for the change.

The request must be approved by the Data Protection Officer, who is also responsible for determining if consent must be sought from the data subject. Where additional consent is required, the Data Protection Officer will determine the form that this consent must take and the process to be followed by the Constabulary in informing the data subject about the new purpose and obtaining the data subject's consequent consent. Where a relevant exemption applies, the Data Protection Officer will identify this exemption in the authorisation to process.
In all cases, the Data Protection Officer is responsible for amending the Data Inventory Record with details of the new purpose, cross-referenced to the Authorisation to Process.

Data Sharing

The Data Protection Officer shall be consulted where personal data is to be shared with a third party organisation.

The Data Protection Officer is responsible for ensuring, where information is to be shared with a third party, that this sharing is compatible with the Constabulary's notification to the ICO, with the Privacy Notice previously made available to the data

subject and with any consent given by the data subject, and that a written agreement is drafted by the Constabulary's legal advisers and entered into by the third party, and that this agreement:

- Describes both the purposes for which the information may be used and any limitations or restriction on the further use of the personal information for other purposes.
- Includes an undertaking from the third party or other evidence of its commitment to processing the information in a manner which will not contravene the GDPR.
- Where the law allows data to be shared without the data subject's consent, the agreement contains specific safeguards/controls to protect the personal information in the context of the GDPR.

The Data Protection Officer is responsible for ensuring, where data collected by the Constabulary is matched with other data to create data profiles, that these profiles are only used within the context of its notification to the ICO and that this is compatible with what the data subject has consented to.

Lawful Basis for Processing

The Constabulary has identified the lawful basis for processing as follows:

For employees (officers and staff, current and prospective) the Constabulary relies on **contractual obligation** arising from the need to process personal data 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 in order to fulfil our contractual obligations under Employment Law.

For former employees the Constabulary relies on **legal obligation** arising from the need to process the personal data to comply with a common law or statutory obligation.

For members of the public the Constabulary will rely on one of the other lawful basis such as **vital interests** where processing is necessary to protect the data subject's life, **public task** where the Constabulary needs to process personal data 'in the exercise of official authority' which covers public functions and powers that are set out in law; or to perform a specific task in the public interest that is set out in law.

The Constabulary does not rely on **Consent** as a lawful basis for processing, except in limited circumstances relating to additional employee benefits and services over which employees have genuine choice and control such as Childcare Voucher and Cycle to Work Schemes. For a full list of consents collected, contact the data protection officer Data.Protection.Officer@cnc.pnn.police.uk

Special category data (such as Occupational Health records) is processed under Article 9 (2) (h) as necessary for the purposes of preventive or occupational medicine and for the assessment of the working capacity of the employee.

The Constabulary processes minimal Criminal Offence data as this is handled by the host Home Office Forces within whose area the sites policed by the Constabulary are based. Where it is processed by the Constabulary this is done on the basis of legal authority under Article 10.

The Data Protection Officer is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the GDPR and as a minimum once per annum.

A current version of this document is available to all members of staff on the intranet.

Change history

Issue	Description of Change	Approval	Date of Issue
1	Initial issue		25/5/18
2	Amended following auditor comments		5/11/18
3	Reviewed following audit		2/2/2020
	Reviewed	DPO	22/01/2021