PERSONAL RECORDS

Owning Department: HR

Department SPOC: HR Policy Manager

Risk Rating: Medium Low

Legal Sign Off: Nichola Thatcher, Deputy Head of Legal Services, 18.09.24

JNCC: September 2024

Published Date: 20/09/2024 (v2.1)

Review Date: 16/09/2024

Index

Legal Basis

Legislation specific to the subject of this policy document:

- UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018
- Freedom Of Information Act 2000

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

- Human Rights Act 1998 (in particular A.14 – Prohibition of discrimination)
- Equality Act 2010

Other documentation which you must check this document against:

- College of Policing – Code of Ethics
- Norfolk and Suffolk Constabularies' Standards of Professional Behaviour
- College of Policing – Authorised Professional Practice

1 Statement of Policy

1.1 The purpose of this policy is to provide guidance and information on the retention and maintenance of, and access to, information held on individuals by the People Directorate in compliance with the UK General Data Protection Regulation and the Data Protection Act 2018. All personal data is processed lawfully, fairly and in a transparent manner and for specified, explicit and legitimate purposes. This policy supplements the Constabularies' Data Protection Policy.

1.2 The organisation explains to data subjects how personal data including special category personal data and criminal records data is used when it collects the data. Please see the Appendix - Fair Processing Notice.

1.3 Norfolk and Suffolk Constabularies (together "the Constabularies") are committed to ensuring this policy complies with relevant legislation and that consultation has been undertaken with all relevant staff groups. Unless we have expressly stated that a policy is contractual (applicable to police staff only) all our policies and procedures are non-contractual. We can change our policies at any time following consultation with UNISON and Federation. Our policies may also be periodically updated to reflect changes in legislation.

1.4 All our policies promote equality, eliminate unlawful discrimination and actively promote good relations regardless of age, disability, gender reassignment, marriage or civil partnership, pregnancy and maternity, race, religion or belief, sex, sexual orientation, economic or family status. Managers have a specific responsibility to ensure this policy is applied fairly, and all officers and staff have a shared responsibility in ensuring the success of this policy.

1.5 This policy has been formally agreed via the approved policy development and review process. It will be maintained by the HR department in conjunction with the Central Policy Unit.

1.6 The Constabularies will review this policy periodically to ensure that it reflects appropriate standards, continues to meet our needs, and reflects any changes in legislation.

1.7 The People Director has overall responsibility for the effective operation of this policy and for ensuring compliance with the relevant statutory framework. Day-to-day responsibility for operating the policy and ensuring its maintenance and review has been delegated to the Head of HR Delivery.

2 Applicability

2.1 This policy applies to current and former:

- Police Officers
- Police Staff
- Special Constables
- Police Support Volunteers
- Casual workers
- External contractor staff
- Job applicants

3 Confidentiality and disclosure

3.1 All official matters or information obtained in the course of work with the Constabularies is strictly confidential, including dealings with and information obtained about current and former officers and staff and members of the public. Such matters must not be discussed with or disclosed to any person outside the police service (including the media) unless the individual is authorised to do so by their line manager, and internal disclosure should only be undertaken when there is an operational or managerial necessity to discharge the individual's responsibilities to the Constabularies.

3.2 Any unauthorised breach of confidentiality is a serious matter that can give rise to disciplinary or misconduct proceedings which could result in dismissal and also carries the risk of a criminal prosecution.

3.3 Any queries about disclosure should be referred to the individual's line manager or the Data Protection team.

4 Personal data records

4.1 Personal data records are those relating to living persons which identify individuals either by the sole means of any record or together with other information that is available to the organisation.

4.2 Personal data is collected, processed and retained on any individual who might wish to work, works or has worked for either of the Constabularies. This includes all computerised and automated personal data records together with any paper and microfiche records, medical records and any financial information, and any supervisor's or line manager's notes relating to individuals.

4.3 Personal data may include information such as:

- Name
- Title
- Address
- Date of birth
- Telephone number
- E-mail address
- Gender
- National Insurance number
- Bank account details, payroll records and tax status information
- Photograph
- CCTV footage and swipe card records
- Salary and grade details
- Records concerning performance and training

- Sickness and other absence details, including information required to process Ill Health Retirement and Injury Award claims
- Annual leave records
- Contract and terms and conditions of employment (police staff only)
- Pension and benefits information
- Start date and, if different, the date of continuous employment
- Leaving date and reason for leaving
- Location of employment or workplace
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process)
- Education
- Work history (including job titles, work history, working hours, holidays, training records and professional memberships)
- Proof of identity, such as a photocopy of birth certificate
- Marital status, family circumstance and dependants
- Next of kin and emergency contact details
- Records of grievances
- Records of disciplinary/misconduct proceedings
- Health and safety records
- Secondary employment and volunteering
- Records of any employment tribunals
- Records of any suspension details
- Records concerning any compensation payments
- Information about your use of Constabulary information and communications systems
- Correspondence with or about an individual

4.4 It is important that personal data held about any individual is accurate and up to date. Individuals must keep the Constabularies informed if their personal information changes during their working relationship with the Constabularies and are responsible for keeping their personal data which is held on the self-service EBS on-line portal up to date (i.e. name, title, address, contact details, next of kin).

5 Special category data and criminal records data

5.1 Special category data is personal data that needs a higher level of protection because it is sensitive. Special category data is personal data revealing or concerning:

- racial or ethnic origin;
- political opinions;

- religious or philosophical beliefs;
- trade union membership;
- genetic data for the purpose of uniquely identifying a natural person;
- biometric data for the purpose of uniquely identifying a natural person;
- physical or mental health;
- sex life or sexual orientation;

5.2 Criminal records data is also afforded a higher level of protection. This is information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

5.3 Special category personal data and criminal records data will only be collected or processed if required for the Constabularies to exercise or perform any right or obligation imposed by law in connection with employment or membership of the Constabularies, or with the explicit consent of the individual.

5.4 A list of HR related purposes for processing special category data is set in the Fair Processing Notice, which includes:

- Equal opportunities monitoring

- information required for equal opportunities monitoring purposes is kept in an anonymised form. Monitoring forms are kept under review to ensure that the information collected is accurate and not excessive.

- Health

- to ensure compliance with health and safety obligations;

- to assess fitness for work;

- to carry out appropriate capability procedures if an officer or member of staff is not fit for work;

- to ensure officers and staff receive the sick pay or other benefits which they may be entitled to;

- to allow the Constabularies to comply with their duties under the Equality Act 2010 for individuals with a disability.

- Racial and ethnic origin

- data related to nationality is processed to ensure that the Constabularies comply with their obligations to check that they are entitled to work in the UK.

- Criminal records data

  - Criminal records data is processed as part of recruitment processes and, where necessary, in the course of employment to verify that candidates are suitable for employment or continued employment and to comply with legal and regulatory obligations to which the Constabularies are subject.

6 Data records held on personal files

6.1 A computerised personal file will be set up and maintained by People Customer Services (PCS) for each officer, police staff employee, and casual worker, with the exception of chief officers. Personal files for chief officers will be held and maintained by each Constabulary's Force Executive team.

6.2 Each personal file held by PCS will retain the following file structure:

- Discipline/Misconduct
- Grievance
- Anti Bullying, Harassment, Sexual Harassment
- Leaver
- Maternity and Paternity
- Medical and Sickness
- Performance Management
- Pre-employment
- Recruitment
- Terms and Conditions
- Other

6.3 All information relating to sickness, including records of any sickness management procedures, Force Medical Advisor (FMA) reports, case conference notes, etc. will be held separately within the Medical and Sickness sub-folder. All other medical information will be held by Workplace Health in line with their own protocol.

6.4 All personal data records in relation to misconduct or disciplinary matters, grievances, unsatisfactory performance and sickness absence management will be retained in line with the relevant force policy.

6.5 Any special category personal data which is not applicable for retention in a designated separate sub-folder, must be retained within a separate area of the personal file, and only processed by PCS where this is necessary for employment rights or obligations.

6.6 No duplicate information should be held on personal files nor should managers hold any local personal files. PCS are responsible for ensuring that documents placed on personal files comply with this policy, the Constabularies' policies on Retention and Disposal and the principles of the Data Protection Act 2018.

6.7 The Constabularies' policies on Retention and Disposal set out the length of time for which documents should be held. Personal data authorised for disposal must always be disposed of as 'confidential waste'.

7 Access to personal files

Subject access to personal files

7.1 All current officers and staff, and former officers and staff, have a right to view their personal file or request a copy of any documents held on file.

7.2 Requests to view a personal file should be made to PCS at PeopleCustomerServices@suffolk.police.uk. The request will be responded to with within five working days of receipt. For current officers and staff, PCS will contact the individual to arrange a mutually convenient appointment to view any paper file, as well as making available any documents held electronically, which may be sent to them via email. Individuals may have both paper and electronic files depending on when they joined the organisation. Requests from former officers and staff will be forwarded with the entire file to the Data Protection Team to manage disclosure.

7.3 Prior to a viewing appointment or sending file documents via email, PCS will inspect the personal file and remove only the following categories of material:

- Information expressly excluded from disclosure by the Data Protection Act, for example information:
  - held for management forecasting or planning (including plans to promote, transfer or make staff redundant);
  - concerning contractual negotiations with any person;
  - contained in references given in confidence (this relates to references given by the Constabularies rather than references received from other organisations);
  - for preventing/detecting crime or apprehending/prosecuting offenders;
  - for the assessment/collection of tax;
- Medical records, which a Force Medical Advisor has decided are not appropriate for disclosure within the terms of the Medical Records Act 1988 or the Access to Health Records Act 1990.

- Information relating to other staff/officers or any third party where disclosure could breach the Constabularies' duty of confidentiality.
- Advice requested of or provided by Legal Services or counsel (this may be marked LLP) may be exempted under the Legal Professional Privilege exemption – advice should be sought from Legal Services or counsel prior to disclosing any such information.

7.4 When viewing a file in person at the PCS office, the individual will be asked to present photo ID on arrival and will be allowed to examine the file in the presence of a member of PCS and make whatever copies or collate whatever notes they so wish.

Requests for access by individuals other than the subject

7.5 Line managers may request access to their team members' personal files for management purposes, which may also include preparing retirement/leaver citations. Line managers should contact PCS to arrange this. The same redaction process under 6.4 will be undertaken. Information may also be provided to managers by email for this purpose where the information is held electronically.

7.6 Requests to receive personal information about officers or police staff will be refused to anyone other than the subject of the information and their line manager unless the Constabularies are legally obliged to provide them, for example where:

- the individual who is the subject of the information makes a request to the People Customer Services Manager that this disclosure be made to a third party, or
- the request arises from a criminal investigation or tax evasion enquiry, or
- the request arises from the investigation of a disciplinary or misconduct allegation, or
- the request is for the transfer of information to other individuals within the Constabularies and is necessary to ensure effective supervision/management, or
- the Constabularies have been ordered to disclose by a court or tribunal or appropriate jurisdiction.

7.7 Generally, employers are under an obligation to disclose specific information to the:

- HM Revenue and Customs;
- shared service providers;
- pension services providers;

- external auditors;
- third party service providers;
- Government Legal Department (GLD).

7.8 If supervisors or managers are in doubt as to the existence of a legal obligation, they must seek advice from the Data Protection Officer before any disclosure of personal data.

7.9 Personal information will not be published about officers or staff (for example identifying details in press articles or force publications) unless there is a legal obligation to do so OR the individual has consented.

8 Correction of records

8.1 If an individual disagrees with the contents of their personal file on the grounds of alleged inaccuracies, incomplete, misleading or out of date information, they should contact their HR Advisor in writing with a detailed explanation and outline the outcome they seek. If the HR Advisor authored the document and agrees with the proposed outcome they will ensure that the record is amended. If the HR Advisor is not the author of the document, then this must be sent to the People Customer Services Manager who will ensure that this is assessed and corrected or annotated in line with Article 16 of UK GDPR and Section 46 of the Data Protection Act.

8.2 If the author of the document disagrees with the proposed outcome, they must record why they disagree and place that record, together with the individual's written report, on the personal file for future reference. If the author of the document is unavailable to comment upon the proposed outcome, a record of this must be made by the HR Advisor, together with the individual's written report, and placed on the personal file for future reference. If the individual continues to disagree with the decision then they should invoke the Grievance policy.

9 Archiving personal files of leavers

9.1 Where the Constabularies retain paper personal files of individuals who leave, these files will be weeded of all unnecessary information and sent to the Off-Site Storage Service Provider where they will be retained in line with the Review, Retention and Disposal of Crime and Non-Crime Related Information Schedule and destroyed at the appropriate interval.

9.2 All electronic files will be weeded by a member of PCS in line with the guidance within the Review, Retention and Disposal of Crime and Non-Crime Related Information Schedule, and marked as such within the file structure.

9.3 The Constabularies are in the process of transferring all paper files to Off-Site Storage Service Provider. These can still be accessed by emailing PeopleCustomerServices@suffolk.police.uk who will request for the file to be returned to the Constabulary.

9.4 All new information will continue to be placed on the electronic files.

10 Retention of recruitment information

10.1 All documentation and electronic records relating to the recruitment and selection process of police officers and police staff, including details of unsuccessful external candidates, will be retained on the Constabularies' OLEEO Recruitment System, and disposed of in line with the force Review, Retention and Disposal Schedule.

10.2 Oleeo will anonymise any pre-screen fails straight away. Any personal data in Oleeo on fails at other stages is anonymised after 12 months and for successful applications, personal data is removed after three years. All information will be lifted from Oleeo and placed in the personal file for those who are employed by the Constabularies.

Fair Processing Notice

Norfolk and Suffolk Constabularies will collect and use personal information so that they can carry out their legal and legitimate functions as defined by legislation, common law, regulation, policy and best practice. The Constabularies hold information electronically and in paper format of all personnel, individuals on a temporary contract, volunteers, members of the Special Constabulary and contractors in accordance with the UK General Data Protection Regulation and the Data Protection Act 2018, and for the following purposes to support policing, including:

Support Functions:

- HR, Pensioner Administration, Occupational Health and Welfare
- Public Relations/ Media
- Finance/ Payroll/ Benefits/ Accounts/ Audits/ Internal Review
- Training/ Health & Safety Management
- Property/ Insurance/ Vehicle/ Systems and Transport Management
- Complaints
- Vetting
- Legal Services/ Information Provision
- Management of information technology systems
- Licensing/ Registration
- Research (including surveys and analytics)/ Performance Management
- Sports/ Recreation
- Procurement
- Planning/ Testing/ Security
- Health and Safety Management
- Strategy and Policy development
- Sale/ Provision or Purchase of Goods and Services
- Social Media Correspondence and analysis

A list of HR related functions is specified as an Appendix to this document.

The Constabularies will collect and use personal information only for employment/contract purposes and will not use or disclose information for any other purposes without your consent, unless required to do so by law, or where the use or disclosure is permitted by law and is necessary and reasonable to do so.

Personal data may include information such as your:

- Name
- Address
- Date of birth

- Telephone number
- Gender
- National Insurance number
- Bank account details and payroll records
- Education
- Work history
- Proof of identity, such as a photocopy of your driving license
- Marital status, family circumstance and dependants
- Next of kin and emergency contact details
- Photograph
- CCTV footage and swipe card records
- Salary and grade details, including data held on staff organograms
- Records concerning your performance and training
- Sickness and other absence details, including information required to process Ill Health Retirement and Injury Award claims
- Annual leave records
- Your contract and terms and conditions of employment
- Correspondence with or about you
- Records of grievances
- Records of disciplinary proceedings
- Health and safety records
- Secondary employment and volunteering
- Records of Employment Tribunals
- Records of any Suspension details
- Records concerning any compensation payments
- Information about your use of Constabulary information and communications systems.

Special category personal data includes information collected for equal opportunities monitoring and may include:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- health
- sexual life
- sexual orientation
- genetic data
- biometric data (where used for identification purposes)

It is important that the personal information we hold about you is accurate and up to date. Please keep us informed if your personal information changes during your working relationship with us.

Where one set of records is relevant to another action, the records may be used for that purpose. For example, absence levels and patterns may be reviewed in connection with unsatisfactory performance policies to establish whether ill health might be a contributing factor. Employment records and records generated by your employment may form part of any unsatisfactory performance, absence management, disciplinary, misconduct or criminal investigation and audit of system use to prevent and detect abuse of Constabulary systems and data.

Identification information e.g. name, date of birth, post number, pay number, collar number, warrant number etc, will be used to allow access to Norfolk and Suffolk Constabularies' information systems.

We may share information with other police forces to assist in decisions relating to recruitment or transfer or conduct issues.

The Constabularies will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you; where it is in the public interest to do so or where it is necessary for the performance of our functions. "Third parties" includes third-party service providers (including contractors and designated agents) and other government departments.

External parties include:

- HM Revenue and Customs
- Shared service providers
- Pension services providers
- External auditors
- Third party service providers
- Government Legal Department (GLD)

This may, in some circumstances, involve sharing special categories of personal data and, where relevant, data about criminal convictions/allegations. The Constabularies may use external contractors to carry out certain policing support functions. Where such a function includes access to and/or use of employment records, the contract will specify the conditions under which that access and use is permitted.

We take care to ensure the information we hold is accurate, up-to-date and deleted when no longer required, in accordance with the force Review, Retention and Disposal Schedule.

The Constabularies will ensure that information is adequately protected through a variety of physical, technological and procedural measures to maintain and safeguard the confidentiality, integrity and availability of the information by preventing unauthorised access and unauthorised or accidental disclosure, loss or corruption.

Personnel are trained in the appropriate procedures and policies for correct handling of personal information.

Access to employment records will be limited to HR and other personnel who have an official purpose for accessing the records. Your line manager and chain of command will generally have access to your employment records for official purposes.

Individuals have a number of rights enshrined in the Data Protection legislation:

- **Right to be Informed**
  This is provided for in Articles 13 and 14 of UK GDPR and Section 44 of the Data Protection Act 2018 which sets out the general duties of a Controller. This Fair Processing Notice addresses that requirement.

- **Right of Access**

  Individuals have the right to apply for a copy of their personal data held by Norfolk and Suffolk Constabularies. This right, commonly referred to as Subject Access is created by Article 15 of UK GDPR and Section 45 of the Data Protection Act 2018 and is used by individuals who want to see a copy of the information an organisation holds about them (subject to exemptions). An individual who requires a copy of their personal information should contact the Data Protection Team to make a Subject Access Request who will ask you to provide a copy of two forms of identification.

  Force policy allows you to request to view your personnel records. Individuals who wish to only view their HR personnel file should make a request to People Customer Services to arrange a mutually convenient appointment and location for the file to be inspected.
  If you wish to obtain a copy of your Occupational Health Records, you can make a request directly to the Workplace Health team.

- **Right to Rectification**

  Article 16 of UK GDPR and Section 46 of the Data Protection Act 2018 provides individuals with the right to have inaccurate personal data rectified or completed if it is incomplete. This may involve the Constabulary providing a supplementary statement to the incomplete data.

Should you find any of the information we hold about you is incorrect or misleading, we will ensure it is thoroughly assessed and corrected/ annotated where appropriate.

- **Right to Erasure**

  Article 17 of UK GDPR and Section 47 of the Data Protection Act 2018 provides individuals with the right to have personal data erased. This is known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances.

- **Right to Restrict Processing**

  Article 18 of UK GDPR and Section 47 of the Data Protection Act 2018 provides individuals with the right to restrict processing of their personal data in certain circumstances. This means that an individual can limit the way an organisation uses their data.

- **Right to Data Portability**

  Article 20 of UK GDPR provides individuals with the right to receive personal data they have provided to a Controller in a structured, commonly used and machine readable format. It also gives them the right to ask a Controller to transmit this data directly to another Controller.

- **Right to Object**

  Article 21 of UK GDPR provides individuals with the right to object to: processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority; direct marketing; and processing for purposes for scientific/historical research and statistics.

- **Rights related to automated decision making including profiling**

  Article 22 of UK GDPR and Sections 49/50 of the Data Protection Act 2018 makes provision to protect individuals from processing carried out solely by automated decision making that has legal or similarly significant effects on them.
  Any individuals with concerns regarding the way in which the Constabularies handle their personal information, may contact the Data Protection Officer, via the following:

  Information Management Department
  Norfolk and Suffolk Constabularies
  Martlesham Heath
  Ipswich
  Suffolk
  IP5 3QS

  Email: compliance@suffolk.police.uk

The Information Commissioner is the independent regulator responsible for enforcing the legislation and provides advice and guidance about the requirements. The Information Commissioner's Office (ICO) can be contacted via the following:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 0303 123 1113 (local rate)
Website: www.ico.org.uk

Appendix to Fair Processing Notice – List of HR Functions:

- Production of management information for internal use and for government bodies as required, e.g. HMIC, Home Office, etc.;
- Maintaining the Force establishment of posts;
- Equal pay reviews and monitoring;
- Job evaluation;
- Recruitment, selection and promotion;
- Deployment activities;
- Managing new starters, leavers and transferees to the organisation;
- Pensions arrangements;
- Reviewing and actioning changes to terms and conditions;
- Providing information to payroll for payment;
- Managing and monitoring sickness, disciplinary, grievance, unsatisfactory performance and flexible working activities;
- Managing and monitoring breaks in service, e.g. maternity, career break, external secondment, etc.;
- Learning and development activities, e.g. training courses, etc.; and
- Responding to legal requests for information, e.g. Employment Tribunal claims, Data Protection requests, Freedom of Information requests etc.