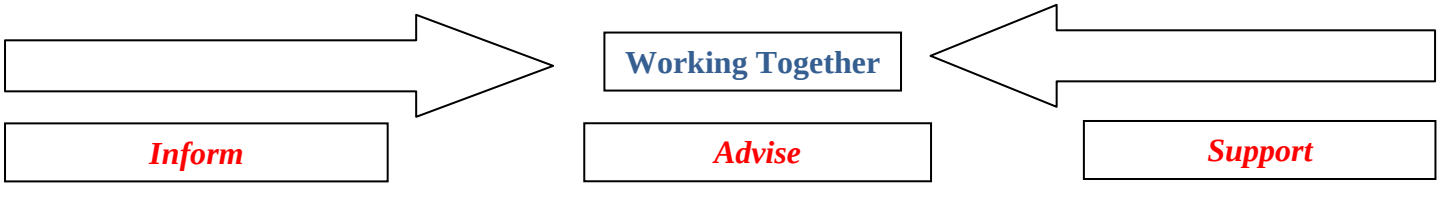
NORFOLK CONSTABULARY
Our Priority is You

SUFFOLK CONSTABULARY
Taking pride in keeping Suffolk safe

JOINT HR POLICY DOCUMENT

PERSONAL RECORDS



NORFOLK CONSTABULARY
Our Priority is You

SUFFOLK CONSTABULARY
Taking pride in keeping Suffolk safe

Personal Records

Force Policy Document

Policy owners	DCC Norfolk / DCC Suffolk
Policy holder	Head of HR Service Delivery (Norfolk & Suffolk)
Author	HR Manager (Policy & Reward)

Policy No.	174

Approved by

Legal Services	N/A
Policy holder	✓
JJNCC	✓

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

Publication date	28/10/2013
Review date	28/10/2016
APP Checked	N/A

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

Index

1 General principles

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 Human Resources department.

1.2 Norfolk and Suffolk Constabularies are committed to ensuring this policy complies with relevant legislation and general principles of fairness, and that consultation has been undertaken with all relevant staff groups.

1.3 All Norfolk and Suffolk policies are intended to promote equality, eliminate unlawful discrimination and actively promote good relations regardless of a person's gender, race, ethnic origin, colour, nationality, gender reassignment, sexual orientation, religion or belief, marital or family status, trade union or staff association or support group activity, disability or age.

1.4 Individuals are able to inspect and correct all the information kept by the Constabularies about them on request, subject to the restrictions as described within the relevant Constabulary Data Protection policy/procedure.

1.5 All official matters or information obtained in the course of work with the Constabularies is strictly confidential, including dealings with and information obtained about colleagues, 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.

1.6 Any unauthorised breach of confidentiality is a serious matter that can give rise to disciplinary proceedings, dismissal and carry the risk of a criminal prosecution.

1.7 Any queries about disclosure should be referred to the individual's supervisor or the Data Protection team.

2 Scope of this policy

2.1 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. They include all computerised and automated personal data together with paper and microfiche records, medical records and any financial information, held in relation to a Health Insurance Scheme and any supervisors' notes relating to individuals.

2.2 Personal records are all data records collected and retained on any individual who might wish to work, works or has worked for either Norfolk or Suffolk Constabularies including:

- applicants (successful and unsuccessful);
- former applicants (successful and unsuccessful);
- employees (current and former);
- agency workers (current and former);
- casual workers (current and former);
- contract workers (current and former);
- volunteers (current and former);
- police officers (current and former);
- members of the Special Constabulary (current and former).

2.3 Sensitive personal data relates to information about:

- racial or ethnic origin;
- political opinions or persuasion;
- religious beliefs or other beliefs of a similar nature;
- trade union membership or affiliation;
- physical or mental health or condition;
- sexual life;
- commissioned or alleged commission of offences;
- any proceedings for any offence, committed or alleged, including any sentencing decisions made by the Court.

2.4 Sensitive personal 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. Recruitment monitoring forms should be destroyed confidentially when the individual is appointed to the role.

2.5 Any sensitive data in the personal file which is not suitable for retention in a separate folder, e.g. medical information, disciplinary information, etc. should be retained within the personal file in a sealed envelope marked 'Sensitive data – only to be opened by a member of the HR Service Delivery team'.

2.6 Personal files for chief officers and those staff employed in the Office of the Police & Crime Commissioner will be held in the Office of the Police & Crime Commissioner.

3 Access to personal files

Subject access to personal files

3.1 Individuals who do not wish to view their file but solely require a full or partial copy of their personal file should contact the Data Protection Office to make a formal subject access request.

3.2 All staff and officers have a right to view their personal file. Requests should be made to the HR Service Desk and will be dealt with within two working days of receipt of the request. HR will contact the individual to arrange a mutually convenient appointment and location for the file to be inspected.

3.3 Prior to the appointment, a member of the HR Service Delivery team 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;
  - held under a duty to investigate disciplinary matters.
- Medical records, which a Force Medical Advisor has decided are 'Not 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.
- Information 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.

3.4 The individual should present photo ID on arrival, and will be allowed to examine the file in the presence of a member of the HR Service Delivery team and make whatever copies or collate whatever notes he/she wishes.

Requests for access by individuals other than the subject

3.5 Line managers may access individuals' personal files for management purposes, which may also include preparing retirement/leaver citations. Line managers should contact the HR Service Desk to make arrangements for this.

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

- the individual who is the subject of the information has requested in writing to the Head of HR Service Delivery that this disclosure be made to a third party, or
- the request arises from an emergency where the individual's best interests are served by disclosing the information (for example to next of kin), or
- the request arises from a criminal 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.

3.7 Generally employers are under a legal obligation to disclose specific information to the:

- Inland Revenue;
- Child Support Agency;
- Benefits Agency;
- Department of Works and Pensions;
- Financial Services Authority.

3.8 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.

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

4 Correction of records

4.1 If an individual disagrees with the contents of their personal file on the grounds of alleged inaccuracies, incomplete, misleading or out of date information, he or she should write to their HR Advisor with a detailed explanation and outline the outcome they seek. If the HR Advisor authored the document and agrees with the proposed outcome he or she will ensure that the record is amended. However, it must be noted that the HR Advisor will not be able to agree changes to a document drafted by someone else. In such instances the individual should liaise, where possible, with the author of the document to seek resolution.

4.2 If the author of the document disagrees with the proposed outcome, he or she 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 should be made by the HR Advisor, together with the individual's written report, and placed on file for future reference. If the individual continues to disagree with the decision then he or she should invoke the Fairness at Work procedure.

5 Information held on personal files

5.1 No duplicate information should be held on personal files. The HR Service Desk is responsible for ensuring that personal files are subject to regular auditing to ensure that content complies with this policy, the Constabularies' policies on Retention & Disposal and the principles of the Data Protection Act 1998.

5.2 All information will be retained in date order with the most recent information at the top of the file. All personal files will include:

- Information relating to original application: copy of recruitment documentation (role profile, job details, advertisement), original application form, interview notes, selection test results (if applicable), details of any relocation payments received, offer letter, pre-employment checks and contract of employment, together with any other relevant information about appointment including any correspondence in relation to starting salary.
- Details of any temporary and/or permanent changes to salary and/or the contract of employment, including all related correspondence explaining the reasons for the change.
- Details of any references provided by the Constabulary.
- Details of commendations or good work recognitions, honoraria, etc.
- Details of breaks in service, i.e. maternity leave, career break, etc. including all related correspondence.
- Details of any compromise agreements made between the individual and the Constabulary.
- All leaving documentation.
- Any other information as deemed necessary.

5.3 All information relating to sickness, including records of any sickness management procedures, FMA reports, case conference notes, etc. should be held separately to the personal file. All other medical information should be held by Occupational Health in line with the Confidentiality Charter at Appendix A.

5.4 All records in relation to disciplinary matters, grievances, unsatisfactory performance and sickness management will be retained in line with the relevant policy.

5.5 Please refer to the Constabularies' policies on Retention & Disposal for guidance on the length of time for which documents should be held. Personal data authorised for disposal will always be disposed of as 'confidential waste'.

6 Archiving personal files of leavers

6.1 Local procedures apply for the management of leavers' personal files:

- **Norfolk:** When an individual leaves the organisation their personal record will be sent to the HR secretariat within six months of their leaving date, by which time all of the necessary leavers check lists must be fully completed. Files should be weeded prior to being archived with any unnecessary information destroyed as confidential waste. The leavers check lists and exit interview/questionnaire will be retained on the personal file. Once weeded, personal files will be retained within HR for two years and then sent to Deep Store.
- **Suffolk:** When an individual leaves the organisation their personal record will be weeded with any unnecessary information destroyed as confidential waste. The leavers check lists and exit interview/questionnaire will be retained on the personal file. Once weeded, personal files will be retained within HR for 12 months and then sent to Deep Store.

7 Storage, transit and communication of personal files and information

7.1 Personal files should only be held by members of the HR Service Delivery team and will only be accessible by members of the HR department for the purposes stated in the Data Handling statement at Appendix B. Storage will comply with Principle 7 of the Data Protection Act, which requires that personal data should be subject to adequate protection from accidental or deliberate loss, damage or destruction.

7.2 Information contained in the personal file should be marked private and confidential as required by the Communications FPD. Personal files and individual documents disclosed should be logged utilising local tracking procedures to ensure that a clear audit trail is available. Personal files will be subject to annual dip sampling by HR to ensure that content complies with this policy and the principles of the Data Protection Act 1998.

8 Retention of recruitment information

8.1 All documentation relating to the successful candidate must be retained on their personal file as detailed in section 5. Details relating to unsuccessful internal applications will be retained on the individual's personal file.

8.2 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 by the HR Service Desk for 12 months after the appointment of the successful applicant.

9 Electronic records

9.1 Electronic records will be held in accordance with the Data Protection Act 1998. Please refer to the following policies for guidance; Information Security, The E-mail and Communicator (IM), Information Management.

Appendix A - Occupational Health Confidentiality Charter

1 Introduction

1.1 All staff in Occupational Health recognise that confidentiality is key to the service that is provided. In order to ensure that this is maintained this Confidentiality Charter has been developed.

2 Occupational Health Records

2.1 Occupational Health information regarding police officers and staff is held in individual Occupational Health (OH) files within the Occupational Health department. These files are securely stored and access is restricted to authorised OH personnel only.

2.2 Overall custodians of the Occupational Health files are the Occupational Health Nurse Advisers (OHNA) and Occupational Health Nurse Manager; due to the fact that the Force Medical Advisors (FMA) are employed on a part time basis only.

2.3 Occupational Health files must not be removed from the department without permission of the Occupational Health Manager. Away from the department, files must be carried in a suitable secure case.

2.4 Information held in an individual's Occupational Health file generally comprises of:

- health questionnaires;
- results of any pre-employment screening, health screening or health surveillance;
- GP or specialist reports;
- reports to management and documentation of any consultations with the OHNA or FMA;
- referral letters to General Practitioners, Specialists, Physiotherapists or other support services;
- management referrals;
- copies of consent forms.

2.5 All written entries in individuals' files are to be legible, written in black ink and initialled, stamped and dated. Specimen signatures are recorded for ease of identifying handwriting of medical and nursing staff.

3 Access to medical files

3.1 Individuals have the right to view or have copies of any information held within their own occupational health file, however, at the discretion of the custodian there is a specific procedure to be followed as below.

3.2 A request by an individual to view their Occupational Health file must be arranged by appointment giving a minimum of 48 hours' notice. On attending OH the individual MUST provide proof of identity. Viewing of any medical information held on file will be under the supervision of the OHNA or FMA. No copying or removal of record(s) is permitted via this process and they will view the file in a supervised environment. There is no fee for this process.

3.3 A request for a copy of all or part of the file must be requested by the individual or their appointed representative (including the Federation's or UNISON's solicitors) by completing the Patient Authority Consent form which is available from Occupational Health.

3.4 Originals will be retained in Occupational Health. All records will be sent by special delivery and marked Personal and Confidential. A subject access request for a copy of OH records will incur a fee of £10.00.

3.5 Information will NOT be released until OH has received the completed Patient Authority Consent form.

3.6 In exceptional circumstances the custodian of the records may limit the individual's access to certain parts of the records, for instance, if information is likely to be detrimental to their wellbeing or relates to another individual.

3.7 Management do not have the right to view any occupational health files or obtain medical information without the informed written consent of the individual concerned.

3.8 The OHNA or FMA cannot obtain medical information from an individual's GP or consultant without written consent from the individual concerned. The individual's rights under this process are informed by the Access to Medical Reports Act 1988 details of which are on the reverse of our consent form. In some cases an entire copy of GP records is requested, for instance to seek permanence of an injury and a similar process of signed consent will be followed.

3.9 Any email/memo/letter or basic management report or guidance that has been sent or e-mailed to a named Human Resources Manager/Advisor or Line Manager is labelled; and **MUST** be treated as Personal and Confidential and only used in relation to the individual to whom it refers. These documents must be handled as RESTRICTED-MEDICAL under the Force Protective marking scheme.

3.10 Any signed consent by the individual allowing information to be obtained or given, is valid for that one episode only and is valid for use within a reasonable length of time, i.e. six months.

4 Confidentiality agreement

4.1 The Occupational Health administration team work closely with the Doctors and Nurses in OH and have access to Occupational Health files. All non medical and non nursing staff within Occupational Health and Safety are required to sign a confidentiality agreement based on an ethical code of practice regarding any medical or personal information. This is to ensure that information of a confidential nature remains within Occupational Health and is not discussed or disclosed inappropriately.

5 Occupational Health Attendance

5.1 One of the key functions of Occupational Health is to monitor and advise on the effects of work on health and health on work. To achieve this aim, certain activities are undertaken, such as:

- Sickness absence monitoring;
- Health screening;
- Health surveillance and accident/injury monitoring or assessment.

5.2 Officers and staff will therefore be required to attend the department for a number of reasons.

6 Management Referral

6.1 This is a referral procedure by which managers (normally Human Resource Managers/Advisors, Recruitment Manager, Line Manager or Supervisor), can request that an individual be assessed by OH.

6.2 Reasons for referral may be because of concerns regarding the individual's ability to fulfil the duties of their post, in compliance with health and safety requirements, or a means of monitoring sickness absence. The manager is required to complete a management referral Form A175 stating the reason for referral and what advice they require from OH. The manager should inform the individual that a referral has been made and reasons why. On receipt of the A175 referral form, OH will arrange for the individual to be contacted and if appropriate, seen as soon as possible.

6.3 Following consultation with the individual, a reply to management will be produced. This may be in the form of a brief e-mail / memo / letter or basic management report, informing management of the individual's functional ability to undertake or continue their work related tasks. No correspondence will be disclosed without the individual's informed consent. In most cases this consent will be written.

6.4 Management will be notified if any individual fails to attend an arranged appointment.

7 Other Occupational Health Contact

7.1 Officers and staff may contact OH to discuss health concerns informally over the telephone, or by e-mail / text. If appropriate, a record of the call or conversation may be entered into the individual's Occupational Health file or noted under a code for statistical purposes.

8 Audit

8.1 Attendance information may be released from the Occupational Health department in the form of statistics and reports, for example, Freedom of Information requests. This is only released if there is no possibility of identifying individuals or groups.

Appendix B - HR Data Handling Statement

This statement is produced to meet the requirements of the Data Protection Act 1998. HR staff (permanent, temporary and agency/contract staff) will collect and use personal information so that it can carry out its legal and legitimate functions as defined by legislation and best practice. We will use the personal information held electronically and on personal files of all of our staff to undertake the full range of HR functions, summarised below:

- 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 and leavers 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.;
- responding to legal requests for information, e.g. employment tribunal claims, Freedom of Information requests, etc.

All personal information will be held and handled in accordance with this policy and the Data Protection Act 1998:

- We will collect and use information only for the above HR functions and will not use or disclose information for any other purposes without the consent of the individual unless required to do so by law.
- We may give information to agents or contractors so that they can provide the facilities we need. In such cases legally binding contracts covering the use and security of information will be put in place.
- We may share information with other agencies under partnership working arrangements. Where personal information is shared, personal details that can identify individuals will be removed where appropriate. We will share personal information only when it is lawful to do so and when the individual's rights have been fully considered.

- We take great care to ensure the information we hold is accurate, kept up to date and is destroyed when no longer required.
- We use a variety of physical, technical and procedural measures to protect personal information from unauthorised or accidental disclosure, loss or corruption.
- Our staff are trained in the appropriate procedures and policies for correct handling of personal information.

We will normally provide a copy of any information we hold about individuals on their request. If an individual believes the information we hold is inaccurate or misleading it will be checked and corrected if appropriate.

If an individual is unhappy with the way in which their personal information has been handled they can complain to the relevant authority as below:

- Information Compliance Manager Suffolk – FHQ Martlesham, extension 3632
- Data Protection & FOI Manager Norfolk – OCC, Wymondham, extension 2806