

Police Service of Northern Ireland

Policy for Public Disclosure.
Procedure and Guidance

HQ Ref: HR/PD012

PD 13/08

POLICY DIRECTIVE

HUMAN RESOURCES (HR) SYSTEM MANAGEMENT POLICY

1. POLICY IDENTIFICATION

POLICY TITLE:	Human Resources (HR) System Management Policy
POLICY OWNERSHIP:	Director of Human Resources (DHR)
DEPARTMENT BRANCH AUTHOR	Human Resources (HR) Personnel – People Development Personnel – People Development
POLICY APPROVED BY:	CCF
CCF REF/OTHER DATE OF APPROVAL	17 December 2007
IMPLEMENTATION DATE:	3 September 2008
DATE OF ISSUE:	3 September 2008
REVIEW DATE:	4 September 2009

INDEX

SECTIONS 1- 6 FOR PUBLIC DISCLOSURE

Section	Subject	Page
1	Policy Identification Page	1
2	Policy Statements	3
3	Introduction	3
3(1)	Executive Summary	3
3(2)	Drivers for Change	3-4
3(3)	Aims	4
3(4)	Legal Basis/Definitions	4-5
4	Implications of The Policy	5
4(1)	Efficiency	5
4(2)	Training	5
4(3)	Internal Policy Links	5-6
4(4)	Risks	6
4(5)	Consultation	6-7
5	Human Rights/Equality/Integrity/Freedom of Information	7
6	Review	7
SECTION 7		
Paragraph	Procedures and Guidance	
1.	HR System Roles	8
2.	HR System Responsibilities	8
3.	HR System, Management of Access	8-14
Appendices		
Appendix 'A'	Data Protection Act 1998	15-16
Appendix 'B'	Computer Misuse Act 1990	17
Appendix 'C'	Official Secrets Act 1911-1918 and 1989	18
Appendix 'D'	HR System Access Request Form	19
Appendix 'E'	HR System User Instructions (Part 1)	20
	Receipt of HR System User Documentation (Part 2)	21
Appendix 'F'	Internally Managed Office Procedure	22-26
Appendix 'G'	Internally Managed Office Procedure – Form IMOP	27

2. POLICY STATEMENTS

- (1) The Human Resources (HR) System is the approved repository for all personnel management information recorded for employees of the Police Service of Northern Ireland (PSNI).
- (2) Records created on the HR System during the course of PSNI business are owned by the PSNI and not by an individual.
- (3) The Chief Constable is the Data Controller for the organisation and delegates the responsibility to manage the information on the HR System to the Director of Human Resources (DHR).
- (4) Human Resources (HR) Planning and Resourcing Unit within HR Department will monitor compliance with this Policy. They will also monitor the performance of the Districts/Departments in implementing the procedures issued in conjunction with this Policy Directive.
- (5) All HR System records should be managed in accordance with the procedures set out in this Policy Directive.

3. INTRODUCTION

(1) Executive Summary

- (a) This Policy Directive identifies the management procedures that will be used to ensure that accurate HR Management Information is captured and maintained in relation to required standards.
- (b) This Policy Directive applies to all users of the HR System to ensure accuracy of records as outlined in the Data Protection Act (DPA).
- (c) All employees should apprise themselves of this Policy and adhere to its guidance.

(2) Drivers for Change

- (a) A review of the HR System undertaken by an external supplier in April 2007 identified some inaccuracies in relation to existing records and procedures for recording and maintaining information on the HR System.
- (b) HR System users had expressed some concerns regarding the accuracy of the information currently held/recorded on the system.
- (c) The current HR System has been in place within PSNI for 7 years and during this time has undergone several significant changes in functionality.
- (d) It is recognised that there is a requirement for corporate guidelines for the users of the HR System, to support the devolvement of the HR function from central to local responsibility.
- (e) The DPA places a duty on organisations to ensure that information is accurate and not excessive. Currently the HR Department is aware that information that should be recorded on the HR System is being held on other databases and stand-alone systems. This information is not searchable and does not form part of the corporate memory of PSNI. The introduction of standardised instructions, QA mechanisms and improved training will increase user confidence in the HR System. This will negate the reliance of some employees on other systems thereby ensuring that the HR System is the single repository for all HR Management information.

- (f) The introduction of Employee Self Service and Management Self Service (ESS/MSS) known as Project Sapphire will mean that employees will be able to administer specific aspects of their own personnel records on the HR System. This will reduce administration and improve accuracy and accountability.

(3) Aims

- (a) To ensure that all HR System users are aware of their responsibilities with regards to the creation and management of HR System records.
- (b) To introduce a Change Control Procedure to ensure that amendments to the HR System are documented and appropriately approved.
- (c) To ensure that systems exist to provide all users with appropriate training in viewing or maintaining information held on the HR System according to their role and geographical placement within the organisation.
- (d) To provide a corporate approach to creating and maintaining records on the HR System across the PSNI.
- (e) To ensure that appropriate processes and resources are put in place to enable compliance with the Acceptable Use Policy (AUP), The Manual of Protective Security (MoPS) and the DPA.
- (f) To introduce a Quality Assurance (QA) role in the District and Departmental HR offices. The Heads of HR will be responsible for implementing QA measures within their respective areas.
- (g) To ensure that systems exist to regularly monitor the integrity of the information held on the HR System in compliance with the DPA.
- (h) To introduce an HR System Transaction Log Monitoring Report to monitor compliance with the AUP and the DPA.

(4) Legal Basis/Definitions

- (a) The terms 'record' and 'data' for the purpose of this Policy refer to personnel management information recorded electronically and in accordance with the definitions as per PSNI Regulations 2005, paragraph 15(2).
- (b) A record is information created, received or maintained by PSNI as part of its day-to-day business and kept as evidence of a decision or action.
- (c) The DPA 1998 provides a legally enforceable framework for the processing of personal data and this encompasses sensitive personal data of which personnel information held on the HR System is an important PSNI category.
- (d) The DPA regulates the processing and storage of personal information and establishes standards that must be met in order to maintain compliance when processing such information.
- (e) Essentially the DPA balances and protects the rights of the subject of the personal data against the potentially opposing objective of processing such personal data by the Data Controller (in this instance the Chief Constable).

- (f) All personal data held by the PSNI must be processed in accordance with the 8 Data Protection Principles (DPP), (see Appendix 'A').

Personal Data shall be:

- (i) processed fairly and lawfully;
 - (ii) obtained and held for a specified and lawful purpose;
 - (iii) adequate, relevant and not excessive in relation to the specified purpose;
 - (iv) accurate, necessary and kept up to date;
 - (v) kept no longer than is necessary for specified purposes;
 - (vi) processed in accordance with the rights of the data subject;
 - (vii) appropriately protected against unauthorised or unlawful processing; and
 - (viii) accidental loss, damage or destruction;
 - (ix) not transferred outside the European Economic Area (EEA) without adequate levels of protection for the rights of the data subject being implemented.
- (g) A User of the HR System is someone who views or maintains records from the HR System, including those who have restricted access for Electronic Self Service (ESS) and Electronic Management Service (EMS) purposes.

4. IMPLICATIONS OF THE POLICY

(1) Efficiency

The introduction and implementation of this Policy will seek to improve the quality of the data held on the HR System. This Policy will bring together all procedures and information available to assist PSNI to effectively manage the records held on the HR System. The need for the HR System to hold accurate records has been addressed in this Policy. When fully implemented this Policy will remove the requirement for nugatory work in recording information in stand-alone databases, and spreadsheets. In addition, by ensuring correct application of the HR System, PSNI will not require licences for other systems currently in use.

(2) Training

- (a) PSNI is committed to developing best practice in relation to training users of the HR System.
- (b) PSNI will provide training to support new and existing users of the HR System.
- (c) Following implementation of this Policy all new users will be required to complete HR System Basic Induction Training at the time access is granted to the HR System.

(3) Internal Policy Links

- (a) All Policy Editors should consider whether information obtained, as a result of their Policy, has an organisational requirement to be recorded onto the HR System.
- (b) All Policies that have reference to the recording of personal, personnel or operational information relating to an employee should consider recording this information on the HR System.

- (c) A consultation option has been entered onto the Audit Tool as part of Policy Directive 1/04 - PSNI Policy, Procedure and Guidance.
- (d) The AUP.
- (e) The MoPS which incorporates:
 - (i) 1.1 Data Protection Act 1998;
 - (ii) 1.2 Computer Misuse Act 1990;
 - (iii) 1.3 Official Secrets Acts 1911-1918 and 1989;
 - (iv) 1.4 Copyright, Designs and Patents Act 1998;
 - (v) 1.5 Freedom of Information Act 2000;
 - (vi) 1.6 Regulation of Investigatory Powers Act 2000.

(4) Risks

This Policy will address the following identified risks:

- (a) Failure to adhere to instructions printed in the HR System Manual;
- (b) Inaccurate management information recorded on the HR System.
- (c) Potential breaches of DPA through:
 - (i) The use of stand-alone computer systems to record HR Management information;
 - (ii) Information not being up to date and accurate.

(5) Consultation

The following have been consulted in preparation of this Policy Directive:

- (a) Senior Officers;
- (b) District Commanders/Heads of Departments;
- (c) Heads of HR;
- (d) Equality and Diversity Officer;
- (e) Human Rights Legal Adviser;
- (f) Employment Lawyer;
- (g) Police College;
- (h) Information and Communication Services (ICS);
- (i) Northern Ireland Public Service Alliance (NIPSA);
- (j) Unite;
- (k) Police Federation of Northern Ireland (PFNI);

- (l) Superintendents' Association of Northern Ireland (SANI).

5. HUMAN RIGHTS/EQUALITY/INTEGRITY/FREEDOM OF INFORMATION

- (1) This Policy is deemed to be Human Rights compliant.
- (2) This Policy has been screened for Section 75 considerations and meets integrity standards.
- (3) This Policy is suitable for publication on the PSNI website thus allowing Public Disclosure in accordance with the Freedom of Information Act 2000.

6. REVIEW

This Policy will be subject to annual review by HR Planning and Resourcing Unit, HR Department. This review will involve appropriate consultation with relevant stakeholders.

SECTION 7

PROCEDURES AND GUIDANCE

1. HR SYSTEM ROLES

- (1) The Chief Constable is designated as the Data Controller for the organisation. For the purposes of the HR System this duty is delegated to the Director of HR.
- (2) HR Planning and Resourcing Unit, HR Department will monitor compliance with this Policy.
- (3) The HR System Administrator will monitor the records and users of the HR System.
- (4) The role of the users of the HR System is to maintain accurate records, and to notify the HR System Administrator of any procedural inaccuracies, which may affect the creation and management of documents.
- (5) An HR System applicant is an employee who is applying for new or increased HR System access.

2. HR SYSTEM RESPONSIBILITIES

- (1) The main responsibility of the users of the HR System is to ensure all information being processed is done so accurately and promptly.
- (2) The users of the HR System should ensure they comply with the guidance set out in this Policy.
- (3) The HR System Administrator has responsibility to the users of the system to ensure that access requests are processed promptly in line with the access criteria.
- (4) The HR System Administrator should ensure that Transaction Log Monitoring is carried out promptly when requested.
- (5) HR Planning and Resourcing Unit within HR Department will ensure this Policy is reviewed within 12 months of the date of implementation.
- (6) Heads of HR should ensure that the all QA processes are complied with.
- (7) Whilst there are specific obligations placed on the Data Protection Unit (DPU) in the organisation, all Heads of HR, Heads of Departments, District Commanders and Heads of Business Service Units must ensure that within their respective business areas, individual line managers who process information understand their own responsibility for data protection compliance. In most cases, practical application of this obligation will fall to the person responsible for HR management in the District/Department.

3. HR SYSTEM, MANAGEMENT OF ACCESS

(1) Accessmaster

- (a) The HR System is accessed via the common terminal and is available through Accessmaster, which determines access based on organisational roles. The Accessmaster role assigns the HR System icon on the desktop but access to the system itself must be applied for separately, via the HR System Administrator in HR Department. When approved, access to the system is achieved automatically via the 'single sign-on' system therefore no typing of a separate user ID and password is required.

- (b) It is important that all User Ids and/or passwords are not shared with others as this could compromise the security of data, and would contravene the AUP and the MoPS and may result in disciplinary action.

(2) Access to the HR System

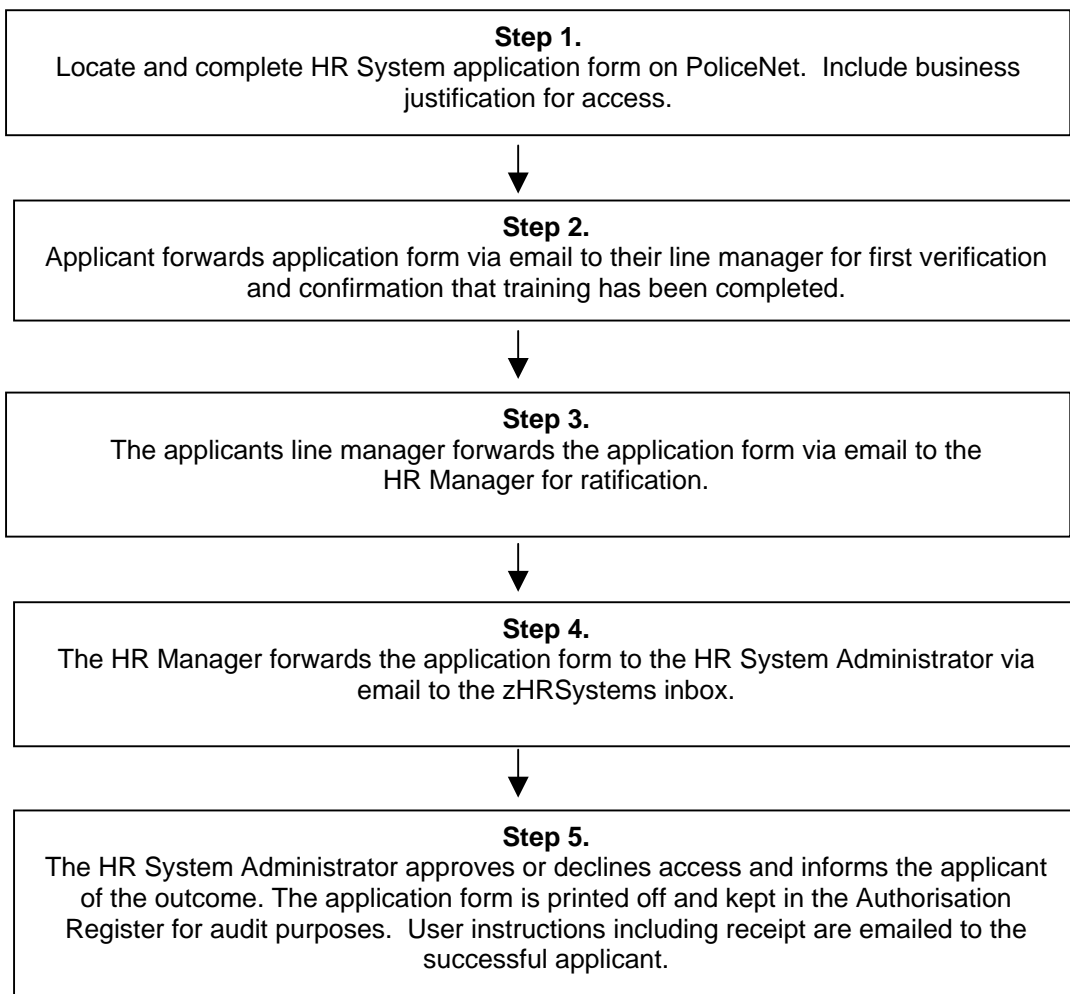
- (a) As a personnel database the HR System holds sensitive personal data relating to all employees and is controlled by the HR Planning and Resourcing Unit within HR Department.
- (b) HR Managers are local 'owners' of the HR information and therefore have an important role in protecting the information for which they are responsible. Therefore, although, all access and control will be the responsibility of the HR System Administrator within HR Department, all requests for access should be submitted via the applicant's line manager and approved by their HR Manager.
- (c) In all cases, but especially outside of the HR function, access will only be granted if it can be proved that a clear and agreed business need exists.
- (d) Access is granted by the HR System Administrator within HR who must determine that:
 - (i) the individual requesting access requires access to the information system for the purpose of carrying out the individual's duties within the PSNI;
 - (ii) the level of access requested is appropriate and the minimum required to perform the job functions;
 - (iii) access will be restricted on a minimum need basis and limited by function and by business/geographical area;
 - (iv) all applications for access will be based on a business need and should be in line with access criteria defined by HR;
 - (v) limited access for specific functions may be granted to individuals where there is a clear need (eg deputising duties);
 - (vi) access to view records on the HR System will only be approved upon completion of HR System Basic Induction Training;
 - (vii) access to add or edit records will only be approved after the applicant completes HR System Basic Induction Training and training relevant to their job discipline.

(3) Access Procedure

- (a) All requests for new or increased access to the HR System should be made by the applicant on the standard HR System Access Application Form (see Appendix 'D').
- (b) The HR System Access Application Form can be found on [Human Resources intranet pages, A-Z, HR system](#) completed and sent by email to the line manager of the applicant for verification.
- (c) When ratified, the line manager should forward the completed form via email to the applicant's HR Manager for secondary ratification.
- (d) The HR Manager must be satisfied that there is a clear business need and that the requested access is appropriate in this case.
- (e) The HR Manager will then forward the request, after completing the relevant detail, to zHRSystems via email.

- (f) The HR System Administrator will, if approved, grant access and ensure such access is commensurate with the effective functioning of the applicant's role and the least access necessary to fulfil that role.
- (g) The HR System Administrator will retain a hard copy of the completed application form for audit purposes.
- (h) On granting of access, the HR System Administrator will forward 'HR System User Instructions' (see Appendix 'E') and, where requested, an induction manual with a receipt that must be completed and returned to the HR System Administrator within 14 working days or access will be terminated.
- (i) The completed receipt will be retained by the HR System Administrator along with the completed application form for audit purposes.
- (j) The HR System User and their line manager will be responsible for identifying any further HR System training required.
- (k) The User is responsible for all usage of the account and will be held answerable for compliance with DPP.
- (l) Line managers and HR Managers will ensure the HR System Administrator is notified immediately when a User is suspended or no longer requires access to the HR System.

FLOWCHART TO SHOW PROCEDURE FOR HR SYSTEM ACCESS APPLICATION



(4) Controls

- (a) A User account will be automatically delimited in the following circumstances:
 - (i) User has not logged on for a period of 6 weeks or more;
 - (ii) User has been transferred, promoted or demoted;
 - (iii) User has left the organisation.
- (b) If the User still requires access they must re-apply using the standard application form, stating the business justification for the restoration of access.
- (c) Continued access is not an automatic right and the HR System Administrator must be satisfied that a clear business need exists, and may alter the level of access in line with the 'least access required' principle.
- (d) Transaction Log Monitoring operates within the HR System, recording changes to data and recording details of individuals who view defined 'sensitive' personal information.
- (e) HR Managers must ensure that all record keeping is accurate and up to date and must ensure that access to personal data is carefully controlled and systematically reviewed.
- (f) Within the context of PSNI, the disclosure of home address or telephone contact details for any employees has particular sensitivity. HR Managers must take steps to ensure that there is no unauthorised access to such details.
- (g) HR Managers will be responsible for ensuring that all those with access to the HR System are aware that they can be criminally liable if they knowingly or recklessly disclose personal information outside of PSNI policies and procedures.
- (h) The bulk of data input and maintenance will be the responsibility of local HR administration.
- (i) Normal 'business as usual' transactions such as change of personal circumstances, absence management, appraisal recording etc, will be the responsibility of the HR Manager.

(5) Security of Computer Printouts and Documentation

- (a) MoPS, paragraph 3.18.1, available for reference on PoliceNet, identifies three types of printout produced by PSNI computer systems:
 - (i) Printouts containing computerised personal information (ie information from which a living individual can be identified);
 - (ii) Printouts containing other non-personal information;
 - (iii) Statistical printouts.
- (b) MoPS, paragraphs 3.18.2 – 3.20.7 outline how printouts obtained from all PSNI computer systems, including the HR System, should be dealt with and users should make themselves familiar with these procedures.
- (c) All printouts produced from the HR System, should be handled in line with the guidelines pertaining to security classification and protective marking, and destruction of this material should be carried out in line with PSNI Retention and Disposal Schedule.
- (d) Users of the HR System should note that much of the information retrieved from the HR System, for example addresses, is classified as 'Confidential' and should be treated accordingly.

(6) Requesting changes to HR System

(a) Raising the Request

- (i) Requests for changes to and enhancements of the HR System should be made via the ICS web portal. As much detail should be given including the information to be recorded/reported on, the business imperative for change and the required timescales for completion.
- (ii) If required, a member of ICS will meet with a representative from the unit with corporate responsibility for the record area to discuss and clarify the requirements for the change. This outline requirement must be approved by the Head of Unit with corporate responsibility for the record area.

(b) Production of Functional Documentation

- (i) ICS will liaise with the external contractor in order to produce a product specification document outlining their understanding of the change request.
- (ii) The product specification will:
 - (aa) outline the resource assessment/ cost for the work requested;
 - (bb) document details of changes required and the potential impact on other areas within the HR System/other IT systems;
 - (cc) detail reports required to support the change;
 - (dd) outline any impact on authorisation levels.
- (iii) ICS will manage the change with the external contractor and will liaise with the business side throughout the process.

(c) Testing

The Head of Unit will nominate a suitable business area to test the changes in both the test and 'live' environments. The nominated testing area will advise the Head of Unit/ICS on how the solution meets business requirements and identify any changes or amendments required. If changes are made these must be tested again in the test environment until the Head of Unit is satisfied that the change to the HR System meets the business requirement. Head of Unit must provide ICS with final approval prior to introducing the change into the live HR System.

(7) QA Procedures for the HR System

The QA Procedure is designed to ensure accuracy of data input onto the HR System. There are 3 processes to be carried out as QA Procedures:

(a) Internally Managed Office Procedure

The Head of HR will, for the purposes of this QA Procedure, assume responsibility as the QA Manager. They may in turn delegate this responsibility to a representative from their office or department who will on a regular basis (minimum of quarterly intervals) check a randomly generated list of all records that have been created or edited in their office. The information for review is available from a report on the HR System called 'Logged Changes in Infotype Data'. Appendix 'F' provides instructions on how to run this report. Appendix 'G' provides a template for recording that the checks have been completed.

(b) Controlled Self Assessment

This involves a cross section of local HR staff working in partnership with a neighbouring HR Office, to confirm information is recorded accurately on the HR System and that the Internally Managed Office Procedure is being completed at a minimum of quarterly intervals.

(c) HR System Transaction Report

- (i) The HR System is monitored by the HR System Administrator to detect any deviation from authorised access and record events that will provide evidence in the event of a security incident being reported;
- (ii) Any concerns regarding unauthorised access should be notified to the HR Administrator immediately in order to affect a suspension of the user's access to the HR System;
- (iii) The HR System Administrator will produce a Transaction Log of the information accessed by the user;
- (iv) The Transaction Log will be sent to the line manager of the user identified as having viewed, added or edited information on the HR System;
- (v) The line manager will complete the Transaction Log form with the user and any corresponding documentation to corroborate the record viewed, added or edited, should be produced to the line manager by the user.
- (vi) The line manager will sign off the Transaction Log Monitoring Form and forward to the HR Administrator, Resourcing Unit, Lisnasharragh;
- (vii) All security breaches or unauthorised access will be notified in the first instance to the HR System Administrator and to the HR Manager of the user concerned for consideration of disciplinary action.

(8) Delivering HR System Training

- (a) Training for all users of the HR System will be undertaken by the Police College.
- (b) HR System training for ICS staff will be arranged and supplied by ICS.
- (c) Users requiring training on the HR System should forward their request to their line manager for consideration against business need. Approved applications should be forwarded to the HR System Administrator by email to zHRSystems. The HR System Administrator will maintain a log of all training requests and liaise with Police College to ensure timely and appropriate level of training.
- (d) HR Managers will be required to ensure HR System Basic Induction training is delivered before full access to the HR System is awarded.
- (e) All formal HR System Training will be recorded on the personnel record of the employee on the HR System.

(9) Training Qualifications Catalogue

- (a) The Police College will own, maintain and manage the Qualifications Catalogue on the HR System, in line with courses available within the Police College prospectus.
- (b) All requests for additional qualifications and courses for the HR System should be sent to the Central Administration Team, Learning Support, Garnerville.

- (c) All approved requests for editing or adding qualifications and/or courses on the HR System will be undertaken by the Police College.

(10) Responsibility for Updating Training Records on the HR System

- (a) In terms of the responsibility for updating training records on HR System, the principle rule will be that the training provider is responsible for the accurate and timely update of the training record. The Police College will therefore be responsible for updating the majority of training information.
- (b) Training delivered at a local/regional level, for example, ANPR, Public Order will be updated by the local/regional HR Manager. Local/regional trainers, on completion of a course, will forward a list of successful police officers or police staff by email to the HR Manager.
- (c) Other training resulting in a recognised qualification, such as external courses provided by NPIA, other Police Services or academic suppliers should be updated at a local level by the HR Manager. The individual should provide the HR Manager with a copy of the certificate for the training course. The HR Manager will update the HR System and then file the certificate on the individual's Personal Record.

(11) HR System Users Manual

- (a) The HR System Users Manual is published on PoliceNet. Follow the pathway to the User Guides:
http://policenet/main-home/human_resources/hr_structure_key_personnel/hr_system.htm
- (b) The HR System Users Manual Master Copy is maintained and updated by the HR System Administrator.
- (c) Any amendments to the processes included in the HR System Users Manual should be notified in the first instance to the HR System Administrator by email to zHRSystems.
- (d) Any amendments to processes in the HR System User Manual will be cascaded to all users by email by the HR System Administrator.
- (3) A hardcopy HR System Users Manual is available in all HR offices. All process amendments must be printed off from PoliceNet by a representative from each office and inserted into the manual replacing the old process for new.

DATA PROTECTION ACT 1998

1. (1) The Data Protection Act (DPA) gives effect to the EC Directive (95/46/EC) on the protection of individuals concerning the processing of personal data and on the free movement of such data. It extends data protection controls to cover certain manual, as well as computerised personal data, and attaches conditions to holding or processing sensitive personal data.

(2) The 8 principles of the DPA 1998 are: Data shall be:
 - (a) Processed fairly and lawfully;
 - (b) Obtained and held for a specified and lawful purpose;
 - (c) Adequate, relevant and not excessive in relation to the specified purposes;
 - (d) Accurate, necessary and up to date;
 - (e) Kept no longer than is necessary for specified purposes;
 - (f) Processed in accordance with the rights of the data subject;
 - (g) Appropriately protected against unauthorised or unlawful processing and accidental damage or destruction;
 - (h) Not transferred outside the EEA without adequate levels of protection for the rights of the data subject being implemented.

2. The 1998 Act introduces new restrictions on the holding and processing of what is termed 'sensitive personal data', ie
 - (1) The racial or ethnic origin of the data subject;
 - (2) His/her religious beliefs or other beliefs of a similar nature;
 - (3) Whether he/she is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992);
 - (4) His/her physical or mental health or condition;
 - (5) His/her sexual life;
 - (6) The commission or alleged commission by him/her of any offence;
 - (7) Any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings.

3. With regards to 'sensitive personal data', in addition to being subject to the eight principles above, at least one of the following conditions must be complied with – there are others, but most relevant in the context of employment are:
 - (1) The worker has given their explicit consent to the processing;
 - (2) The processing is necessary for the purposes of exercising or performing any right or obligation, which is conferred or imposed by law on the employer in connection with employment.

4. Particular attention should be paid to Section 55 of the DPA 1998, specifically 55. 1 - a person must not knowingly or recklessly, without the consent of the data controller:
 - (1) Obtain or disclose personal data or the information contained in personal data; or
 - (2) Procure the disclosure to another person of the information contained in personal data.

COMPUTER MISUSE ACT 1990

1. The Computer Misuse Act (CMA) came into force on 29 August 1990.
2. The Act provides provision for securing computer material against unauthorised access or modification.
 - (1) Clause 1 of the Act creates the offence of 'basic hacking' ie unauthorised access to computer resources which consists of 'causing a computer to perform any function with intent to secure access to any program or data' when the access is 'unauthorised' and the person having access 'knows that is the case'.
 - (2) Clause 2 provides that a person is guilty of an offence if he commits an offence under Clause 1 (the unauthorised access offence) with the intent to commit or to facilitate the commission of, any offence for which sentence is fixed at law or would attract a custodial sentence of 5 years or more if committed by a person over 21 not having any previous conviction.
 - (3) Clause 3 creates the offence of unauthorised modification of computer material. A person commits this offence if he causes an unauthorised modification of the contents of a computer with the requisite intent and knowledge.

With particular reference to the PSNI, measures and guidelines must be established to raise awareness and understanding of the Act and it's implications. In particular, all staff must fully understand what is meant by 'unauthorised'. Additionally, procedures must also be established which clearly identify that which is indeed 'unauthorised', and further set out what actions are 'authorised'.

OFFICIAL SECRETS ACT 1911-1918 AND 1989

1. The Official Secrets Acts (OSA) exists to protect information and other assets relating to security, intelligence, crime, defence or international relations from unauthorised disclosure.
2. An offence under OSA is also committed if, without lawful authority any information or other article is disclosed which:
 - (1) Results in the commission of an offence;
 - (2) Facilitates an escape from legal custody or any other act prejudicial to the safekeeping of persons in legal custody;
 - (3) Impedes the prevention or detection of offences or apprehension or prosecution of suspected offenders; or
 - (4) Would be likely to lead to any of these effects.
3. It is also an offence to disclose information obtained under the terms of an interception warrant issued under Section 5 of the Regulation of Investigatory Powers Act, (RIPA) 2000 or disclose anything relating to methods used to obtain such information.
4. It is a criminal offence under the OSA to fail to take reasonable care of PSNI Assets protected by the OSA or fails to comply with official directions regarding their return or disposal.

HR SYSTEM USER INSTRUCTIONS

1. The practice and procedures outlined below are to protect the confidentiality and integrity of the personal information stored on the HR and are to be followed at all times. Users will abide by these procedures as well as all other relevant directives eg.
 - (1) MoPS;
 - (2) AUP.
2. Any breach of these policies and procedures is a disciplinary offence. Additionally, those liable may also may be subjected to criminal charges under the following legislation:
 - (1) Data Protection Act, 1998;
 - (2) Computer Misuse Act, 1990;
 - (3) Official Secrets Act, 1911-1989.
3. Users must acquire proper authorisation from the HR System Administrator before attempting to access the system.
4. **User Responsibilities:**
 - (1) The account is assigned specifically for administrative work;
 - (2) Any unauthorised use of the account for personal purposes, or any other purpose not related to the PSNI is strictly forbidden;
 - (3) Always sign off your account when not using it;
 - (4) Never leave your account logged on and unattended;
 - (5) It is the user's responsibility to keep any password secure to prevent unauthorised access to the account;
 - (6) Do not reveal your password to another individual, even if that person has the same access to the HR System as you have;
 - (7) Position the screen to minimise viewing by unauthorised persons who may be present when information is being retrieved;
 - (8) Clear all accessed information from the screen immediately after obtaining it, to prevent unauthorised viewing of the data;
 - (9) You are prohibited from divulging any administrative data to another individual unless that individual is also authorised to use the data;
 - (10) Only designated offices may release personal data to bodies external to the PSNI.

RECEIPT OF HR SYSTEM USER DOCUMENTATION

HR System Administrator

I have received a copy of the 'HR System User Instructions'.

I have read and I understand the responsibilities of registered users of the HR System.

I am aware that any breach of the policies and procedures may result in disciplinary/ criminal action.

I am aware of the HR System User Guide available on PoliceNet

Signed: _____

Print Name: _____

Date: _____

Rank/Grade: _____

District/ Dept: _____

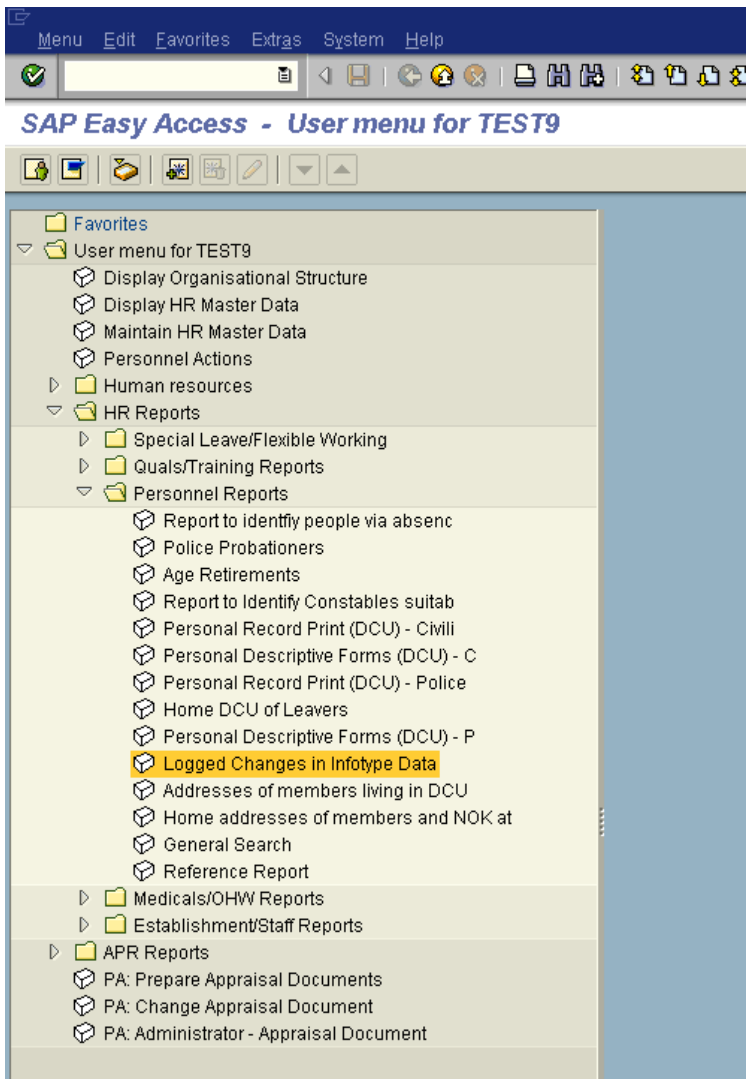
Location: _____

Print out part 'E', Return of User Documentation, and post to:

HR System Administrator,
Resourcing Unit,
Lisnasharragh.

INTERNALLY MANAGED OFFICE PROCEDURE

A report exists under **HR Reports** and then **Personnel Reports** in the SAP Easy Access menu called 'Logged changes in infotype data' Personnel Reports.

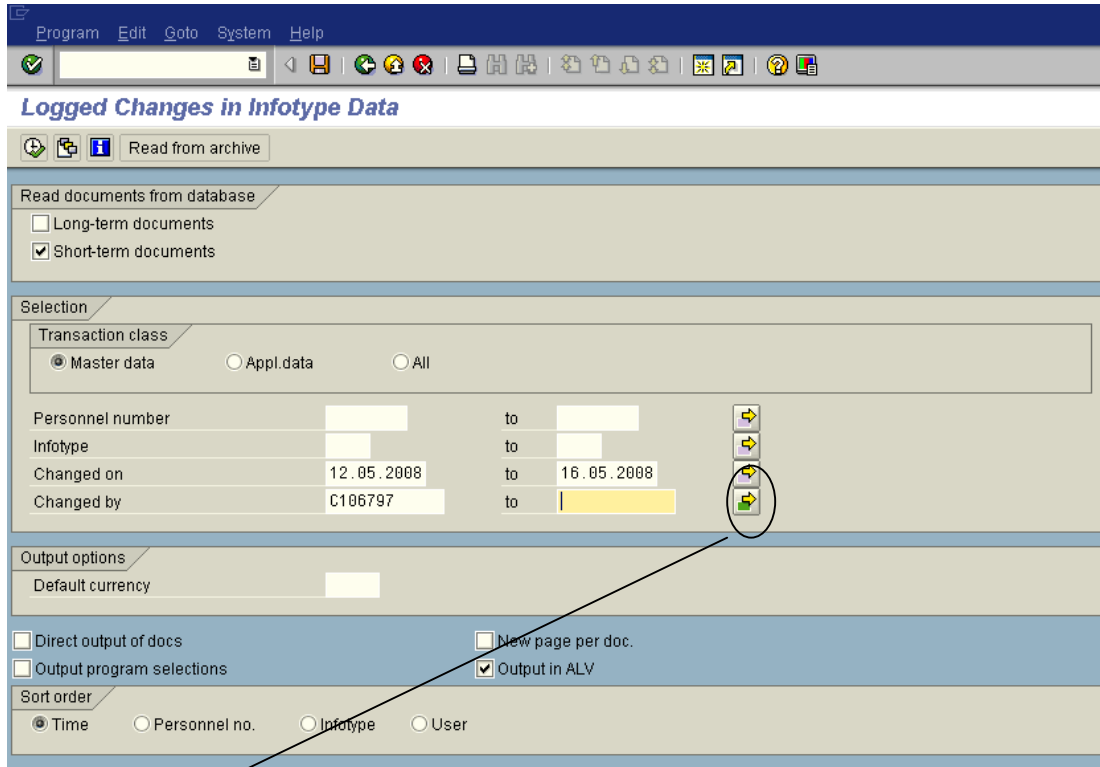


In the selection screen click on 'Short term documents'.

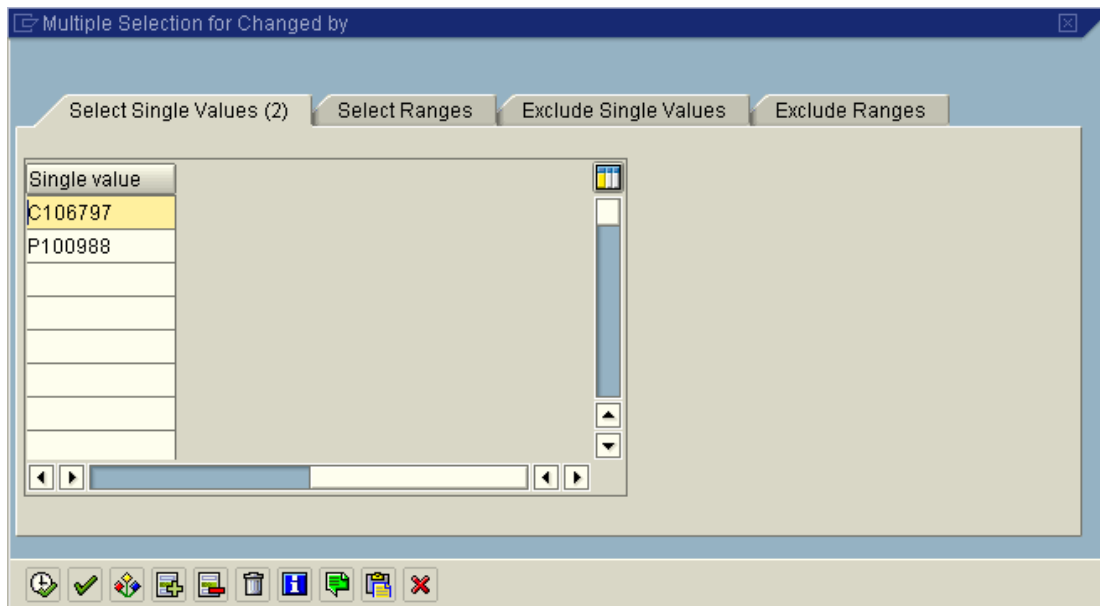
You can limit the report by infotype (screen) eg medical screen is 9082; Addresses is 0006, Personal Data is 0002 (see list below).

The date that the records were changed on or who they were changed by.

For monitoring purposes you should enter a date range you want to report on and the user IDs of your staff:



By clicking on the yellow arrow you can enter multiple user IDs.



The report output gives you a basic list of Dates and times and which screen was amended for which individual and by which user and can be downloaded to MS Excel in the normal way eg:

Date	Time	No.	Pers.No.	Tr.Class	Infotype	User Name
25.02.2008	16:46:32	1	99999	A	0000	JOHNM
25.02.2008	16:46:32	1	99999	A	0302	JOHNM
25.02.2008	16:48:39	1	99999	A	0002	JOHNM
25.02.2008	16:51:13	1	99999	A	0000	JOHNM
25.02.2008	16:51:13	1	99999	A	0002	JOHNM
25.02.2008	16:51:13	1	99999	A	0302	JOHNM
25.02.2008	17:07:03	1	77701	A	0000	JOHNM
25.02.2008	17:07:03	1	77701	A	0302	JOHNM
25.02.2008	17:07:46	1	77701	A	0002	JOHNM
25.02.2008	17:08:00	1	77701	A	0001	JOHNM
25.02.2008	17:08:02	1	77701	A	0019	JOHNM
25.02.2008	17:08:03	1	77701	A	0019	JOHNM
25.02.2008	17:08:03	2	77701	A	0019	JOHNM
25.02.2008	17:08:04	1	77701	A	0019	JOHNM
25.02.2008	17:08:06	2	77701	A	0019	JOHNM
25.02.2008	17:08:06	1	77701	A	0019	JOHNM

If you need specific detail about a particular change go back to the selection screen and narrow your search to the specific date of change; the specific person, the specific screen and individual who made the change eg see below:

Program Edit Goto System Help

Logged Changes in Infotype Data

Read from archive

Read documents from database

Long-term documents

Short-term documents

Selection

Transaction class

Master data Appl. data All

Personnel number 77701 to

Infotype 0016 to

Changed on 25.02.2008 to 25.02.2008

Changed by JOHNMM to

Output options

Default currency

Direct output of docs

Output program selections

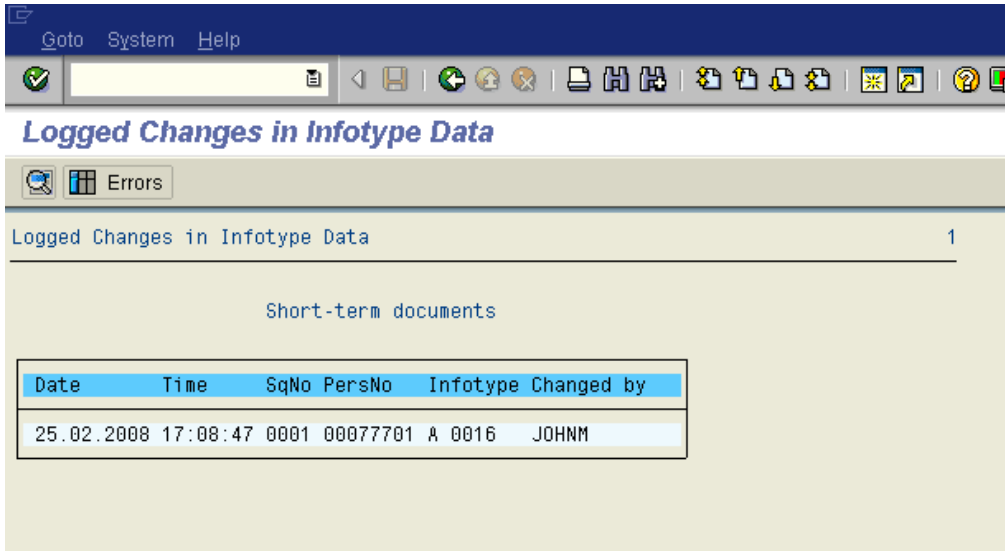
New page per doc.

Output in ALV

Sort order

Time Personnel no. Infotype User

Also be sure to take out the tick in the 'Output in ALV' box. The output comes out like below:



Highlight the entry and click on the 'magnifying glass' and it brings up more detail:

Logged Changes in Infotype Data

PersNo 00077701 77701 : J SHEPHARD
 Infotype A 0016 Contract Elements
 Changed by JOHNM
 Date 25.02.2008 Time 17:08:47 Seq. no. 0001

Subty	Obj	Lck	From	To	No	Old record changed	Action
Field name	Old field					New field	
			01.04.2007	31.12.9999	000		I
Text ex.							
Ref.exists							
CF exist							
Screen control							
Reason							
Grp Value							
SidelineJob							
Com.Clause							
*PCP						0	
PCP							
*SpecRule						00	
*Sick Pay						0	
KGZZH							
*Prob. Per.						0	
PRBEH							
ER NP							
EE NP							
*Work Perm.						00.00.0000	
*Init. Entry						00.00.0000	
*Grp. Entry						00.00.0000	
Group Key							
*Cont. Type						FT	
*Val. Until						31.12.9999	
EE group							
EE subgrp							
Wrk Locat.							
*ContractSt						00.00.0000	
Contr. -no							
*Contract						00	
*Extension						00	
P/T flag							
*Full Pay						000	
*Pension						000	
Rep. Month							

All the fields on the left hand side with an '*' beside it denotes that something has been changed.

Under Action at the top 'I' means 'Insert' so a new record has been entered; 'D' means delete and 'U' means update.

Police Service of Northern Ireland



HR System

**Internally Managed Office Procedure.
(Form IMOP1)**



Date	Employee Name for record edited	Personnel Number for record edited	Infotype edited	Name of Data Editor	Personnel Number of Data Editor	Name of User conducting the IMOP	Personnel Number of user conducting the IMOP	Was the information recorded accurately?