ACPO & ACPOS National Vetting Policy For the Police Community

Document Classification

NOT PROTECTIVELY MARKED

August 2010

VERSION 3.0

Document Approval

Version	Date	Author	Approved by
Version 1.1	18 December 2003	Peter Boylan (GMP) Bob McCaughan (Kent)	ACPO National Vetting Working Group
Version 1.2	21 January 2004	Peter Boylan (GMP) Bob McCaughan (Kent)	ACPO Professional Standards Committee
Version 1.3	14 April 2004	Peter Boylan (GMP) Bob McCaughan (Kent)	Chief Constables' Council
Version 2.1	4 January 2006	Peter Boylan (GMP) Bob McCaughan (Kent)	ACPO National Vetting Working Group
Version 2.2	December 2006	Alan McCawley (Met) Bob Lane (Warwickshire) Carol Benton (Lancashire) Jonathan Gupta (Staffordshire)	Not approved - removed for revision by ACPO PSC
Version 2.3	January 2007	Alan McCawley (Met) Bob Lane (Warwickshire) Carol Benton (Lancashire) Jonathan Gupta (Staffordshire) Stewart Finlayson (Strathclyde)	Not approved
Version 2.4	May 2007	Alan McCawley (Met) Bob Lane (Warwickshire) Carol Benton (Lancashire) Jonathan Gupta (Staffordshire) Stewart Finlayson (Strathclyde)	Not Approved
Version 2.5	July 2007	Alan McCawley (Met) Bob Lane (Warwickshire) Carol Benton (Lancashire) Jonathan Gupta (Staffordshire) Stewart Finlayson (Strathclyde)	Not Approved
Version 2.6	November 2007	Alan McCawley (Met) Bob Lane (Warwickshire) Carol Benton (Lancashire) Jonathan Gupta (Staffordshire) Stewart Finlayson (Strathclyde)	Not Approved
Version 2.7	January 2008	Alan McCawley (Met) Bob Lane (Warwickshire) Carol Benton (Lancashire) Jonathan Gupta (Staffordshire) Stewart Finlayson (Strathclyde)	Not Approved
Version 2.8	February 2008	Alan McCawley (Met) Bob Lane (Warwickshire) Carol Benton (Lancashire) Jonathan Gupta (Staffordshire) Stewart Finlayson (Strathclyde)	Not Approved
Version 2.9	May 2008	Alan McCawley (Met) Bob Lane (Warwickshire) Carol Benton (Lancashire) Jonathan Gupta (Staffordshire) Stewart Finlayson (Strathclyde)	Not Approved
Version 2.10	September 2008	Alan McCawley (Met) Bob Lane (Warwickshire)	Not Approved

		Carol Benton (Lancashire) Jonathan Gupta (Staffordshire) Stewart Finlayson (Strathclyde)	
Version 2.11	November 2008	Alan McCawley (Met) Bob Lane (Warwickshire) Carol Benton (Lancashire) Jonathan Gupta (Staffordshire) Stewart Finlayson (Strathclyde)	Not Approved
Version 2.12	July 2009	Alan McCawley (Met) Bob Lane (Warwickshire) Carol Benton (Lancashire) Jonathan Gupta (Staffordshire) Stewart Finlayson (Strathclyde) Lee Warhurst (Hampshire)	Not Approved
Version 2.13	January 2010	Bob Lane (Warwickshire) Carol Benton (Lancashire) Jonathan Gupta (Staffordshire) Stewart Finlayson (Strathclyde) Lee Warhurst (Hampshire)	Not Approved
Version 2.14	May 2010	Bob Lane (Warwickshire) Carol Benton (Lancashire) Jonathan Gupta (Staffordshire) Stewart Finlayson (Strathclyde) Lee Warhurst (Hampshire)	ACPO Cabinet
Version 2.15 (Final Publication Version 3.0)	July 2010	Bob Lane (Warwickshire) Carol Benton (Lancashire) Jonathan Gupta (Staffordshire) Stewart Finlayson (Strathclyde) Lee Warhurst (Hampshire)	ACPO Cabinet ACPOS Council

POLICY OWNERSHIP:	**ACPO Professional Standards Committee**
POLICY IMPLEMENTATION DATE:	**1st August 2010**
VERSION IMPLEMENTATION DATE:	**1st August 2010**
POLICY REVIEW DATE:	**12 months post implementation by ACPO NVWG**

1. Policy Statement

1.1 The Police Community is committed to the maintenance of the highest levels of honesty and integrity, and to the prevention of; corrupt; dishonest; unethical or unprofessional behaviour. The purpose of the ACPO / ACPOS National Vetting Policy for the Police Community, hereafter referred to as the NVP, is to support that commitment by creating an understanding of the principles of vetting in the police community, thereby establishing uniformity in vetting procedures.

1.2 A consistent application of this NVP will allow police officers, police staff, partner agencies, contractors, or other non-police personnel, to transfer or operate within different forces[1] or agencies with a minimum of duplication of vetting procedures, whilst maintaining high professional standards.

1.3 Personnel Security Vetting is an important process for enhancing the integrity and security of the police community. However, it is based on a 'snapshot in time' and must form part of a wider ongoing protective security regime.

1.4 Following the HMIC report 'Raising the Standard' it is the view of both the ACPO and ACPOS Professional Standards Committees that each force should have a central Force Vetting Unit. In addition, they should appoint a Force Vetting Officer to co-ordinate and control all vetting processes within their force and to adhere to the ACPO / ACPOS NVP.

1.5 This policy identifies the minimum standards that forces should adopt to ensure a consistent approach across the Service. It will only be fully effective if it is adopted by all forces.

2. Procedure

2.1 There are two types of vetting procedures in operation within the police community:

i) **Force Vetting** – Includes Recruitment Vetting (RV), Management Vetting (MV), and Non-Police Personnel Vetting (NPPV).

Force vetting procedures must be underpinned by the completion of the police Authentication Standard Operating Procedure (SOP 2).

ii) **National Security Vetting** (NSV) - Includes Counter Terrorist Check (CTC), Security Check (SC), and Developed Vetting (DV).

Authentication and the relevant level of Force Vetting must be completed prior to any level of NSV being commenced (see SOP 6).

2.2 NSV procedures are underpinned by the HMG Baseline Personnel Security Standard (BPSS). However, the BPSS, on its own, is not an acceptable level of clearance for the requirements of the ACPO/ACPOS NVP. It should be noted that Authentication, when supported by Recruitment Vetting (RV) or

[1] In the context of this policy, reference to 'forces' also refers to police agencies. References to 'Police Officers' includes members of the Special Constabulary and references to 'Police Staff' includes Police Community Support Officers (PCSO's) and Force Support Officers (FSO's) in Scotland.

NPPV 2/3, incorporates all aspects of the BPSS. Therefore, authentication must be completed prior to the NSV procedure being initiated.

2.3 Force Vetting and NSV are separate processes, designed to counter specific threats. The purpose of Force Vetting is to specifically provide a level of assurance, which NSV cannot provide, as to the integrity of individuals who have access to sensitive criminal intelligence, financial, or operational police assets or premises. The purpose of NSV is to protect sensitive government national security assets, by providing an acceptable level of assurance as to the integrity of individuals who have access to protectively marked government assets and/or who require access to persons, sites and materials, at risk of terrorist attack.

2.4 Force Vetting Units should develop a Review, Retention and Disposal schedule for vetting material. This should be developed in line with the requirements of the Management of Police Information (MOPI), the Data Protection Act (DPA) and the Security Policy Framework (SPF).

3. Application

3.1 In the application of this policy and associated Standard Operating Procedures, hereafter referred to as SOPs, the police community will not unlawfully discriminate against any persons regardless of age, disability, gender, transgender, sexual orientation, race, colour, language, religion, political, or other opinion, national or social origin, association with national minority, property, birth, belief or other status as defined under Article 14, European Convention on Human Rights (ECHR). Consideration has also been given to the compatibility of the policy and related procedures with the Human Rights Act; with particular reference to the legal basis of its precepts; the legitimacy of its aims; the justification and proportionality of the actions intended by it; that it is the least intrusive and damaging option necessary to achieve the aims; and that it defines the need to document the relevant decision making processes and the outcome of actions.

3.2 Police officers, police staff, partner agencies, contractors, or other non-police personnel and those working voluntarily or under contract to UK police forces must be aware of and are required to comply with this ACPO / ACPOS NVP.

4. Ownership

4.1 This policy is owned by the ACPO Professional Standards Committee and managed by the ACPO National Vetting Working Group. All decisions made by any ACPO/ACPOS Portfolio relating to the application / introduction for specific groups of vetting must be ratified by the ACPO National Vetting Working Group prior to implementation.

5. Associated Documents and Policies

- ACPO National Vetting Policy for the Police Community V1/V2
- Management of Police Information (MoPI)
- HMG Security Policy Framework (SPF)
- Home Office Circular (HOC) 06/2003
- National Police Improvement Agency (NPIA) Circular 01/2010

- CESG InfoSec Standards inc. Memorandum 22
- Equality Impact Assessment
- Freedom of Information Assessment
- HMIC Report 'Raising the Standard'

- SOP 1 – Vetting Levels and their relevance to the Government Protective Marking Scheme
- SOP 2 – Authentication
- SOP 3 – Recruitment Vetting
- SOP 4 – Management Vetting and Enhanced Management Vetting
- SOP 5 – Non-Police Personnel Vetting
- SOP 6 – National Security Vetting
- SOP 7 – Vetting Interviews
- SOP 8 – Convictions and Cautions Criteria
- SOP 9 – Appeals and Review Procedure
- SOP 10 – Aftercare and Renewal of Clearance
- SOP 11 – Transferees and Re-joiners
- SOP 12 – Career Breaks
- SOP 13 – Other Force Vetting Checks (IMPACT Nominal Index and PND)
- SOP 14 – Reciprocal Vetting
- SOP 15 – Business Interests and Secondary Working.
- SOP 16 – Risk Assessments – Third Party
- SOP 17 – Adverse Information and Judicial Findings (TAINT)
- SOP 18 – Financial Vetting
- SOP 19 – Glossary of Terms and Abbreviations

ACPO Professional Standards Committee

Standard Operating Procedure Number 1

VETTING LEVELS and their relevance to the GOVERNMENT PROTECTIVE MARKING SCHEME

Protective Marking	NOT PROTECTIVELY MARKED
Publication Scheme	Yes
Title	Vetting Levels
Version	3.0
Summary	This Standard Operating Procedure supports the ACPO / ACPOS National Vetting Policy for the Police Community
Management	ACPO National Vetting Working Group
Author	Carol Benton [Lancashire], Stewart Finlayson [Strathclyde], Jonathan Gupta [Staffordshire], Bob Lane [Warwickshire], Alan McCawley [MPS]
Date created	August 2010
Review date	August 2011

1. Introduction

1.1 This Standard Operating Procedure (SOP) supports the ACPO/ACPOS National Vetting Policy for the Police Community (NVP) and associated documents and policies.

1.2 This is a new SOP.

2. Application

2.1 This SOP comes into force on 1st August 2010.

3. Purpose

3.1 The purpose of this SOP is to provide an introduction into the various levels of vetting carried out by the police service and to align them with the Government Protective Marking Scheme (GPMS).

3.2 At Appendix 1 is a summary of the information below.

4. Process

4.1 The principles of GPMS were adapted for police use and adopted by ACPO and ACPOS as an integral part of the ACPO/ACPOS Information Systems Community Security Policy.

4.2 In the police community the classifications to be used are: **NOT PROTECTIVELY MARKED**, **PROTECT**, **RESTRICTED**, **CONFIDENTIAL**, **SECRET** and **TOP SECRET**.

4.3 The protective marking of 'police data' should not be confused with 'government marked data'. This can be addressed by the correct use of descriptors. This will assist in defining the correct level of vetting clearance applicable.

4.4 Whilst accepting the GPMS classifications, as well as the use of descriptors i.e. **RESTRICTED – POLICY**, **SECRET – STAFF** etc., it is extremely important that the recipient of protectively marked police data is aware of the origin of the document. It is recommended that the descriptor 'POLICE' is used when protectively marking police data. i.e. **RESTRICTED - POLICY - POLICE, SECRET - STAFF – POLICE** etc. This will make police data instantly recognisable and avoid the misapprehension that those who require access to 'SECRET' material must be vetted to Security Check (SC) level. In relation to 'police data' Management Vetting (MV) would be more appropriate.

4.5 It should be noted that National Security Vetting (NSV) outside the police community does not incorporate any aspects of Force Vetting, other than reference to the PNC. Thus, reassurances regarding criminality cannot be provided. It therefore follows that the holder of an SC clearance carried out by a non police organisation should not automatically be entitled to view / be entrusted with protectively marked 'police assets'.

5. Authentication

5.1 Authentication, whilst not a formal security clearance, underpins all levels of Force and National Security Vetting.

5.2 Authentication is used to confirm an individual's:
- Identity;
- Nationality;
- Employment eligibility;
- Residency qualification.

5.3 The Baseline Personnel Security Standard ('BPSS') is a specific level of clearance within Her Majesty's Government (HMG). However, the BPSS, on its own, is not an acceptable level of clearance for the requirements of the ACPO/ACPOS NVP. All aspects of the BPSS have been incorporated within the Authentication SOP 2, other than references, which are included in the Recruitment process.

6. Force Vetting Levels

6.1 Recruitment Vetting (RV)

6.1.1 There are no national guidelines in respect of police staff recruitment. However, due to the increasingly wide range of duties carried out by police staff, and resultant access to information, assets and premises, the vetting criteria for the recruitment of police officers and members of the Special Constabulary has been extended to include persons applying for police staff vacancies.

6.1.2 It is fully acknowledged that police officers and police staff owe high standards of duty to the state, and must expect to be subject to scrutiny before they are entrusted to have access to sensitive information or police assets, including premises.

6.1.3 A comprehensive list of the checks required for an RV clearance is given in the RV SOP 3. Certain aspects of the vetting process, whilst owned by the Force Vetting Unit (FVU), can be performed by Recruitment / HR Departments.

6.1.4 Successful completion of RV, which must be preceded by Authentication, allows regular access to protectively marked assets up to and including CONFIDENTIAL and occasional access to SECRET police and government assets. Completion of these two procedures will satisfy all requirements of the BPSS.

6.2 Management Vetting (MV) and Enhanced Management Vetting (EMV)

6.2.1 Management Vetting (MV) specifically relates to those individuals who will be required to undertake posts within designated sensitive areas. The purpose of MV is to provide a means of ensuring that persons serving in 'designated posts', which are those with access to sensitive police information, intelligence, financial or operational assets, have been assessed as to their reliability and integrity. The procedure therefore serves to reduce the risks of unauthorised disclosure, or loss of, sensitive police assets.

6.2.2 There are two levels of MV: Management Vetting (MV) and Enhanced Management Vetting (EMV). It is recommended that all persons with long term, frequent and

uncontrolled access up to SECRET, and occasional access to TOP SECRET police assets, should hold MV clearance. Those who require long term, frequent and uncontrolled access to TOP SECRET police assets should hold EMV clearance. The EMV procedure has been developed to formalise the recommendation made in Version 1 of this policy that additional checks should be added to the MV procedure to counter specific threats.

6.2.3 However, MV and EMV clearances are a requirement for service in all 'designated posts', irrespective of whether post holders have access to police or government protectively marked assets. e.g. those awarding contracts or handling sensitive financial assets.

6.2.4 A comprehensive list of the checks required for MV and EMV is given in SOP 4.

6.3 Non Police Personnel Vetting (NPPV)

6.3.1 The purpose of 'Non Police Personnel Vetting' (NPPV) is to provide a means of ensuring that persons other than police officers, police staff and members of the Special Constabulary, having physical or remote access to police premises, information, intelligence, financial or operational assets have been assessed as to their reliability and integrity. The procedure serves to reduce the risks of unauthorised disclosure or loss of sensitive police assets.

6.3.2 There are three levels of NPPV, Level 1, 2 and 3 and further details of the checks required for each are given in SOP 5.

7. National Security Vetting (NSV) Levels

7.1 Counter Terrorist Check (CTC)

7.1.1 A CTC clearance is required for those individuals who are to be appointed to posts which:

- involve proximity to public figures who are assessed to be at particular risk from terrorist attack;
- give access to information or material assessed to be of value to terrorists;
- involve unescorted access to certain military, civil, industrial or commercial establishments assessed to be at risk from terrorist attack.

7.1.2 For the police, this means all police officers, members of the Special Constabulary, police staff (including Force Support Officers) and non-police personnel whose work involves access as described above. Individuals serving in SC and DV designated posts will be CTC cleared as part of those processes.

7.1.3 It is not intended that all Police Personnel should be CTC cleared as a matter of course. However, it is important that individual forces assess all posts within their force and identify those which fall within the criteria in 7.1.1 and subject only these to CTC clearance. The decision as to whether a CTC is required for an individual is a matter for the Chief Officer.

7.2 Security Check (SC)

7.2.1 An SC clearance is required for those individuals who are to be appointed to posts which:

- require long term, frequent and uncontrolled access to government assets marked SECRET;
- require occasional, supervised access to government assets marked TOP SECRET (such as Chief Constable's Staff Officer and Special Branch staff);

and for individuals who:

- while not in such posts, will be in a position to directly or indirectly bring about the same degree of damage;
- will have sufficient knowledge to obtain a comprehensive picture of a SECRET plan, policy or project;
- are being considered for appointment where it would not be possible to make reasonable career progress without security clearance for access to government assets marked SECRET;
- need access to certain levels of protectively marked material originating from another country or international organisation;

7.2.2 An SC clearance should not normally be required for:

- occasional access to government assets marked SECRET in the normal course of business or during conferences, briefings or courses;
- custody of a small quantity of government assets marked SECRET;
- entry to an area where government assets marked SECRET are stored;
- work in areas where government information at SECRET and TOP SECRET might be overheard;
- use of equipment capable of handling government information marked SECRET, provided that access controls are in place.

In the above circumstances, the BPSS, or Authentication supported by RV or NPPV level 2 or 3 should usually be sufficient.

7.3 Security Check Enhanced (SC (Enhanced))

7.3.1 Where an SC clearance is required for access to SECRET STRAP material, a review of personal finances must be carried out. This may be referred to as an SC (Enhanced) clearance.

7.4 Developed Vetting (DV)

7.4.1 A DV clearance is required for those individuals who are to be appointed to posts which:

- require frequent, uncontrolled access to government assets marked TOP SECRET or require any access to TOP SECRET STRAP, ATOMIC or other codeword material;

and for individuals who:

- while not in such posts, will be in a position to directly or indirectly bring about the same degree of damage;
- require frequent, uncontrolled access to Category I nuclear material;
- need access to certain levels of protectively marked material originating from another country or international organisation.

7.4.2 A DV clearance should not normally be required for:

- occasional, supervised access to limited quantities of government assets marked TOP SECRET in the normal course of business or during conferences, briefings or courses;
- custody of a small quantity of government assets marked TOP SECRET;
- entry to an area where government assets marked TOP SECRET are stored;
- work in areas where government information at TOP SECRET might be overheard;
- use of equipment capable of handling government information marked TOP SECRET, provided that access controls are in place;
- access to SECRET STRAP material only;
- police officers and police staff in posts where there is a threat from serious organised crime, provided that Management Vetting (MV) (SOP 4) is applied and ongoing management of the clearance is augmented by an Annual Security Review.

In the above circumstances, an SC clearance should usually be sufficient.

8. Responsibilities

8.1 This SOP is owned by the ACPO Professional Standards Committee.

8.2 Responsibility for implementing and reviewing the SOP rests with the ACPO National Vetting Working Group.

9. Associated Documents and Policies

- ACPO/ACPOS National Vetting Policy for the Police Community
- Security Policy Framework (SPF)
- Government Protective Marking Scheme
- Authentication SOP 2
- Recruitment Vetting SOP 3
- Management Vetting and Enhanced Management Vetting SOP 4
- Non-Police Personnel Vetting SOP 5
- National Security Vetting SOP 6

ACPO Professional Standards Committee

Standard Operating Procedure Number 2
AUTHENTICATION

Protective Marking	NOT PROTECTIVELY MARKED
Publication Scheme Y/N	Yes
Title	Authentication
Version	3.0
Summary	This Standard Operating Procedure supports the ACPO / ACPOS National Vetting Policy for the Police Community
Management	ACPO National Vetting Working Group
Author	Carol Benton [Lancashire], Stewart Finlayson [Strathclyde], Jonathan Gupta [Staffordshire], Bob Lane [Warwickshire], Alan McCawley [MPS]
Date created	August 2010
Review date	August 2011

1. Introduction

1.1 This Standard Operating Procedure (SOP) supports the ACPO / ACPOS National Vetting Policy for the Police Community (NVP) and associated documents and policies.

1.2 This is a new SOP.

2. Application

2.1 This SOP comes into force on 1st August 2010.

2.2 Authentication, when supported by Recruitment Vetting (RV), incorporates all aspects of Her Majesty's Government (HMG) Baseline Personnel Security Standard, hereafter referred to as BPSS and is therefore a prerequisite for all levels of Force Vetting and National Security Vetting (NSV).

2.3 Authentication is not a level of vetting within the ACPO/ACPOS NVP and is administered by HR or other appropriate sponsor.

3. Purpose

3.1 Authentication is used to confirm an individual's:
- Identity;
- Nationality;
- Employment eligibility;
- Residency qualification.

3.2 Authentication does not allow access to police protectively marked assets or unescorted access to any police premises.

3.3 The BPSS is a specific level of clearance within HMG. However, the BPSS, on its own, is not an acceptable level of clearance for the requirements of the ACPO/ACPOS NVP. All aspects of the BPSS have been incorporated within this Authentication SOP, other than references, which are included the Recruitment process.

4. Process

4.1 Authentication is fundamental to all levels of Force and National Security Vetting and must be completed before any other enquiries are initiated.

4.2 **It is the responsibility of the Recruitment Manager, employer or other internal sponsor to ensure Authentication takes place and is fully audited prior to vetting forms being forwarded to the Force Vetting Unit.**

4.3 The Authentication process comprises four stages that should be carried out in the order shown. Between each stage the information collected should be reviewed and assessed. The stages are as follows:

- Identity Check;
- Nationality Check;
- Employment Eligibility;
- Residency Qualification;

The following information, with the exception of paragraphs 7.1 – 7.5 and 7.8 – 7.10 can be found in HMG's Security Policy Framework (SPF) and the BPSS. For further details please consult these documents.

5. Identity Check

5.1 Verification of identity is essential before any individual can begin their appointment. Identity can be verified by physically checking a range of appropriate documentation (e.g. passport or other photo ID together with utility bills, bank statements, etc).

5.2 The increasing availability of good quality false documentation makes establishing identity difficult; particularly so if un-trained and busy line managers are expected to spot sophisticated fraudulent documents. However, unless identity is confirmed, any other checks that might be undertaken become meaningless.

During the recruitment process, and in advance of any firm offer of appointment, individuals must, as a minimum, be asked to provide:

• Confirmation of name, date of birth and address;

• National Insurance number or other unique personal identifying number where appropriate;

• Full details of previous employers (name, address and dates);

• Confirmation of any necessary qualifications/licences;

• Educational details and/or references when someone is new to the workforce when these are considered necessary;

• Confirmation of permission to work in the UK (a separate verification of nationality and immigration status should still be carried out prior to the commencement of appointment and must be undertaken if an excuse against a civil penalty liability is to be obtained by the employer.) This information must be checked to ensure that there are no obvious gaps and that it is consistent by cross-referencing the data provided.

Useful identifying documents

5.3 The individual's full name and signature, date of birth and full permanent address should be corroborated using as many of the following qualifying documents as is considered necessary on a case-by-case basis. If, in exercising risk management, the required level of assurance can be obtained by the production of a single document, this must include a photo of the individual. Any photograph or identifying information (such as date of birth indicating age) contained in the corroborating document should be compared with the physical appearance of the individual.

Where a signature has not been provided (e.g. because of an e-application) the individual should be asked to provide it at a later date (e.g. at interview) for checking against relevant documentation. It is also good practice to request the same documentation the subject presented at interview on the first day of appointment.

Only original documents should be used for identification purposes. Copies are not acceptable.

• Current signed full passport, travel document National ID Card and/or other documentation relating to immigration status and permission to work (see further guidance in the 'verification of nationality and immigration status' section of this SOP);
• Current UK photo-card driving licence (www.dvla.gov.uk);
• Current full UK driving licence (old version);
• Current benefit book or card or original notification letter from the Department for Work and Pensions (DWP) confirming the right to benefit;
• Building industry sub-contractor's certificate issued by Her Majesty's Revenue and Customs (HMRC);
• Recent HMRC tax notification;
• Current firearms certificate;
• Birth certificate (issued within 6 weeks of birth);
• Adoption certificate;
• Marriage certificate;
• Divorce, dissolution or annulment papers;
• Civil Partnership certificate;
• Recent original utility bill or certificate from a utility company confirming the arrangement to pay for the services at a fixed address on prepayment terms;
• Local authority tax bill (valid for current year);
• Bank, building society or credit union statement or passbook containing current address;
• Recent original mortgage statement from a recognised lender;
• Current local council rent card or tenancy agreement;
• Court order.

5.4 There is no definitive list of identifying documents and not all documents are of equal value. The ideal is a document that is issued by a trustworthy and reliable source, is difficult to forge, has been dated and is current, contains the owner's name, photograph and signature, and itself requires some evidence of identity before being issued (e.g. a passport).

5.5 Where individuals do not have photo ID, they should be asked to provide additional identifying documents from the list. Where they are unable to provide adequate identifying documents (e.g. because of age, lack of residence, etc), departments and agencies should exercise discretion taking into account all other material obtained through the recruitment process. Where this appears genuinely to be a problem, the individual should be asked to provide a passport sized photograph of him/herself endorsed on the back with the signature of a person of some standing in the individual's community (e.g. a JP, medical practitioner, officer of the armed forces, teacher, lecturer, lawyer, bank manager, civil servant, etc) and accompanied by a signed statement, completed by the same person, stating the period of time that the individual has been known to them (minimum 3 years). The statement itself should always be checked to ensure that the signature matches the one on the back of the photograph and that it contains a legible name, address and telephone number. The signatory should be contacted to confirm their status and check that he or she did, in fact, complete the statement.

5.5 In circumstances where verification of identity was not straightforward but a decision is nevertheless taken to appoint the individual(s), departments and agencies must accept and record any associated risk.

6. Nationality Check

6.1 Verification of nationality and immigration status (including an entitlement to undertake the work in question) is required. Nationality and immigration

status can be verified by physically checking appropriate documentation or, in exceptional circumstances only, by means of an independent check of UK Border Agency (UKBA) records. Departments must take the necessary steps to ensure that an individual has the right to remain in the United Kingdom and undertake the work in question.

The Immigration, Asylum and Nationality Act 2006

6.2 Immigration and nationality checks are based on the current provisions on preventing illegal migrant working in the UK as set by the Immigration, Asylum and Nationality Act 2006. These provide that an employer may be liable for a civil penalty by employing someone subject to immigration control aged over 16 who does not have permission to be in the UK or to undertake the work in question. An employer may establish an excuse against this civil penalty liability by undertaking specific documentary checks on the individual before the employment commences in accordance with the Immigration (Restrictions on Employment) Order 2007. Further details and a list of the documents required to establish a statutory excuse can be found at: http://www.ukba.homeoffice.gov.uk/sitecontent/documents/employersandsponsors/preventingillegalworking/currentguidanceandcodes/civilpenaltiescode2008.pdf

Whilst government departments and agencies may have no civil penalty liability because of crown immunity, they are still required to undertake all appropriate document checks. Where the individual has a limited entitlement to remain in the UK, repeat checks should be undertaken not less than twelve months after the previous check was undertaken or, if sooner, before the previous leave has time expired. This will ensure that migrant workers will not be able to continue working after their leave has expired up until the next annual check. These checks will not be required once the appointee can demonstrate that he or she has indefinite leave to be in the UK by producing appropriate documents or the appointment comes to an end. Documents that demonstrate that the employer has established an excuse from a liability for appointing an illegal migrant worker must be retained during the period of employment and for not less than two years after the employment has come to an end.

Comprehensive and summary guidance for employers is available electronically on the preventing illegal working pages of the UK Border Agency website This includes images of immigration documents and two Codes of Practice (on the civil penalty and how to prevent illegal working whilst avoiding unlawful discrimination). It also contains further information on the Workers Registration Scheme and Bulgaria and Romania Authorisation Scheme. Further guidance is also available in the Home Office's 'Comprehensive guidance for UK employers on changes to the law on preventing illegal working.'
http://www.bia.homeoffice.gov.uk/sitecontent/documents/employersandsponsors/preventingillegalworking/
The UKBA provides support to employers through its Sponsorship and Employers' Helpline and Employer Checking Service. It is recommended that employers read the available online guidance before using these services. Further details can be found at
http://ukba.homeoffice.gov.uk/employers/employersupport/

Departments should be aware that the employment of migrants from outside the European Economic Area (EEA) and Switzerland is subject to the points-

based system. Further information about the new system can be found at: http://www.bia.homeoffice.gov.uk/employers/points/

Checks need to be applied evenly, and employers will need to be aware of their obligations under the Race Relations Act. For example, all individuals should be required to provide this evidence and not just those who appear to be migrants. Individuals should be asked to complete the Nationality and Immigration Status Check Form at Annex C, and departments and agencies should corroborate the information against the required document or documents listed in the guidance referred to in paragraph 6.2. The document(s) should be copied, and the copies retained by the department or agency, as explained above.

Immigration employment enquiry (via UKBA)

6.3 Where an individual's nationality and immigration status cannot otherwise be verified or where the check has been carried out and concerns remain, an independent check of UKBA records may be carried out. Such checks should be carried out on an exceptional basis only where other information/documentation already supplied by an individual is insufficient for the need.

Where such a check is necessary, departments and agencies should contact UKBA's Evidence & Enquiry Unit (E&E) by telephone or fax as shown below. For queries relating to the processing of requests, departments should telephone E&E on 0208 196 3003.

• For telephone enquiries, departments and agencies must register with E&E before requests for immigration status information can be accepted. To register, departments and agencies must write to E&E on departmental/agency headed paper to the following address:

Home Office UK Border Agency

Evidence & Enquiry Unit

12th Floor, Lunar House

40 Wellesley Road

Croydon CR9 2BY

http://www.bia.homeoffice.gov.uk/

As well as the request for registration, the letter must also include contact names and telephone numbers. E&E will keep a list of all those registered. Departments and agencies are responsible for ensuring that their registered contacts are up to date. Following registration, E&E can be contacted on 0845 6012298 for all enquiries about whether an individual has a right to work in the UK.

• For fax enquires, departments and agencies must complete the standard request form at Annex D and fax it to E&E on 0208 196 3046 or 3047. E&E will provide a response by fax within a minimum of 28 days of receipt.

• An e-mail address also exists for registered users to send in requests via e-mail. The e-mail address is Pre-employment@indhomeoffice.gsi.gov.uk.

Please note that following the Cabinet Secretary's review of Data Handling Procedures in Government, all requests sent and received by this box must be encrypted, UKBA currently uses PGP encryption software.

In some cases, where a department or agency makes a telephone request, E&E will need to investigate further as to whether an individual has a right to work in the UK. If this is the case, E&E will endeavour to respond within 28 days, as with faxed requests. If departments and agencies require further information about an individual following the 'right to work' check, E&E may be able to provide that information. Any further enquires should be made to E&E in the first instance.

Verification of Immigration and Nationality documentation – sources of further guidance

6.4 'A Guide to the Detection of Passport Fraud' – Advice from the National Document Fraud Unit (part of the UKBA) to help in the detection of forged travel documents. It is a basic introduction to the subject of passport fraud and is aimed at those departments and agencies which are presented with identity documents in the course of their work. The 'Guide' is a Microsoft PowerPoint-based self-managed learning CD Rom which can also be used as the basis of a trainer-led presentation and is normally available to HMG and some corporate bodies only. Further information about the 'Guide' is available from:

UK Border Agency
National Document Fraud Unit
PO Box 1000
Harlington
Hayes
Middlesex UB3 5WB

The Guide forms the basis of the Document Verification Guidance produced by the Centre for the Protection of the National Infrastructure (CPNI) which can be accessed at:
www.cpni.gov.uk/Docs/Documentverification_guidance_released_July_2007.pdf

Information about UK immigration stamps, visas, letters and endorsements can also be found on the UK Border Agency website at:

www.bia.homeoffice.gov.uk/sitecontent/documents/employersandsponsors/preventingillegalworking/currentguidanceandcodes/comprehensiveguidancefeb08.pdf

The European Union launched in 2007 the PRADO website or Public Register of Authentic Documents Online. It contains images and information relating to passports, visas, residence permits, driving licences and other identity and travel documents issued by EU member states. This includes details of their first level security features and how to check their authenticity. The website is available in all the official languages of the EU and can be accessed at:

www.consilium.europa.eu/prado/EN/homeIndex.html

A version for control authorities called iFADO containing a higher level of information on False & Authentic Documents Online is also being rolled out

across the government secure internet. Details about this can be obtained from the National Document Fraud Unit.

• The Identity and Passport Service (IPS) was established as an Executive Agency of the Home Office on 1 April 2006. The Agency builds on the strong foundations of the UK Passport Service (UKPS) to provide passport services and in the future, as part of the National Identity Scheme, ID cards for British and Irish nationals resident in the UK. Foreign nationals resident in the UK will also be included by linking the scheme to biometric immigration documents. The IPS runs the 'OmniBase Service' which provides a web interface into their database of issued passports. It allows, at cost, verification of an individual's passport and a check of its status. Approved departments and agencies will be able to operate the programme using an internet browser. Further information is available from:

Paul Goldsmith
Identity and Passport Service
Allington Towers, 4th Floor
19 Allington Street
London, SW1E 5EB
(0203 356 8112 or Paul.Goldsmith@ips.gsi.gov.uk)
http://www.ukps.gov.uk

7. Residency Criteria/Checkable History

7.1 The residency criteria in the NVP applies equally to all applicants. Where the applicant has resided abroad due to the fact that they have been serving in the British armed forces or on UK Government Service, they are considered to have been resident in the UK. For such individuals, in addition to the checks outlined in the NVP, enquiries should also be made with the Ministry of Defence (MOD) or relevant Departmental Security Officer.

7.2 The purpose of the residency rule arises from the requirement to vet all applicants in an equitable manner. This is due to the fact that the UK Police Service does not currently have any means of facilitating vetting enquiries overseas to the extent required for those who have been resident in the UK. **National Police Improvement Agency (NPIA) Circular 01/2010 very clearly states that applicants who cannot be vetted cannot be appointed.**

7.3 The purpose of the residency criteria is to ensure that applicants have a "checkable history" in the UK to assist Chief Constables in discharging their obligation to run an efficient and effective force. Additionally, the criterion provides some reassurance when considering the Health and Safety of their staff and the public. Neither duty can be fulfilled if the Chief Constable is incapable of assessing the honesty, integrity and reliability of their appointees against the information, or lack of information, available.

7.4 For Force Vetting, the following minimum periods for UK residency apply:

Recruitment Vetting 3 years,
Management Vetting 5 years,
Non Police Personnel Vetting 3 years.

7.5 The calculation of the periods of time shown above, and below, refer to the period immediately before an application is made, and not any other 3, 5, or 10 year period, or any other accumulation of time spent in the UK.

7.6 For NSV, the SPF paragraph 58 sets out the minimum periods of residence in the UK required before meaningful checks at the various national security vetting levels can be completed. Departments and agencies are advised to exercise discretion when individuals have not resided in the UK for the following periods:

- CTC 3 years,
- SC 5 years,
- DV 10 years.

Whilst discretion can be exercised in extreme cases, the overriding principle must be to adhere to the minimum periods set out in Para 7.4.

7.7 Where it is possible to make vetting enquiries in overseas jurisdictions, it is viable for the minimum residency period for Force Vetting levels to be removed. However, this can only be done where it is possible to make checks in the relevant jurisdictions with local Law Enforcement and National Security bodies, which are equivalent to the enquiries which would be made in the UK, on both the applicant and all family members and associates, as detailed within the ACPO/ACPOS NVP. This is in relation to Force Vetting only and does not apply to National Security Vetting.

7.8 In cases where it is not possible to make the equivalent checks, the residency criteria must be stringently enforced. However, it has been recognised in both the associated Equality Impact Assessment of this policy and Council's legal opinion, that whilst the Policy is not directly discriminatory, there may be an element of indirect discrimination, albeit justifiable on the grounds of law enforcement and national security.

7.9 It is further recognised that in the wider policing arena, outside of the vetting community, there is an imperative for the composition of the police service to reflect the communities it serves. Therefore, in **EXCEPTIONAL** circumstances, the Chief Officer of a force may elect to depart from strict application of the residency criteria. Such departure requires the authority of the Chief Officer of the relevant force and **MUST** follow the submission of both a business case and full risk assessment conducted on an individual case by case basis i.e. no blanket appointments will be permissible.

7.10 Despite the appointment being made with Recruitment Vetting clearance having been granted, the individual's subsequent ability to transfer between forces could be jeopardised as the decision to appoint will have been made according to local need and based on the risk appetite of the initially appointing Chief Officer. It is also unlikely that any higher levels of vetting clearance under either the Police or NSV regimes will be attainable until the individual is able to satisfy the residency criteria.

7.11 It should be noted that even where a checkable history can be obtained for those who do not meet the minimum residency criteria, National Security Vetting enquiries may not be possible and therefore Force Vetting Officers should give careful consideration as to whether or not National Security Vetting clearance can be granted.

8. Responsibilities

8.1 This SOP is owned by the ACPO Professional Standards Committee.

8.2 Responsibility for implementing and reviewing the SOP rests with the ACPO National Vetting Working Group.

9. Associated Documents and Policies

- ACPO / ACPOS National Vetting Policy for the Police Community
- Security Policy Framework (SPF)
- Baseline Personnel Security Standard
- Home Office Circular 06/2003
- Recruitment Vetting SOP 3

ACPO Professional Standards Committee

Standard Operating Procedure Number 3
RECRUITMENT VETTING

Protective Marking	NOT PROTECTIVELY MARKED
Publication Scheme Y/N	Yes
Title	Recruitment Vetting
Version	3.0
Summary	This Standard Operating Procedure supports the ACPO / ACPOS National Vetting Policy for the Police Community
Management	ACPO National Vetting Working Group
Author	Carol Benton [Lancashire], Stewart Finlayson [Strathclyde], Jonathan Gupta [Staffordshire], Bob Lane [Warwickshire], Alan McCawley [MPS]
Date created	August 2010

Review date	August 2011

1. Introduction

1.1 This Standard Operating Procedure (SOP) supports the ACPO/ACPOS National Vetting Policy for the Police Community (NVP) and associated documents and policies.

1.2 This is a new SOP.

2. Application

2.1 This SOP comes into force on 1st August 2010.

2.2 Recruitment Vetting (RV) is the initial vetting process for police officers, police staff and members of the Special Constabulary and is the minimum level of check acceptable to ensure access to police assets, estate and information.

2.3 RV should also be applied to 30+ retention officers, police cadets and internal applicants changing employment group i.e. Police Staff becoming Police Officer. This is due to the significant change in role and circumstances, resulting in increased access to information and assets and unrestricted movement in premises and increase in designated powers. Police Officers retiring and rejoining as Police Staff should also be vetted, due to the possible elapse of time since their last renewal.

2.4 There is one level of Recruitment Vetting.

2.5 The authentication procedure (SOP 2) must be completed prior to RV being initiated. At present satisfactory Force Vetting checks abroad cannot be achieved. It is essential that vetting criteria applies to all applicants, thus when such checks can be carried out to the same extent that they are in the UK then residency criteria / checkable history would not be a bar to recruitment. The rationale behind the residency criteria / checkable history is given in SOP 2, together with a description of the provisions relating to the permissible departure from this, in exceptional circumstances.

2.6 RV clearance, preceded by authentication, will allow regular access to police and government assets up to CONFIDENTIAL and occasional access to SECRET.

3. Purpose

3.1 The purpose of RV is to protect the community and the organisation by ensuring that only those who demonstrate the highest standards of conduct, honesty and integrity are recruited or appointed.

3.2 The requirements for Police Officer Recruitment are outlined in National Police Improvement Agency (NPIA) Circular 01/2010, entitled, 'Police Officer Recruitment-Eligibility Criteria for the role of Police Constable'. This includes guidance on the checks to be undertaken prior to the acceptance of applicants. These include qualifications, nationality, finances, criminal convictions, and references. Forces should support each other in ensuring the integrity of the police recruitment process, by carrying out such checks as requested following a positive trace on the IMPACT Nominal Index (INI), or as a result of an LIO check in forces that do not fully upload to INI (see SOP 13).

3.3 It should be noted that the convictions/cautions criteria set out in NPIA Circular 01/2010 does not fully satisfy the requirements of this policy. A revised convictions/cautions

criterion is set out in SOP 8 which should be followed in order to assist Chief Officers in discharging their responsibility to run an efficient and effective police force.

3.4 There are no national guidelines in respect of police staff recruitment. However, due to the increasingly wide range of duties carried out by police staff, and resultant access to information, assets and premises, the vetting criteria for the recruitment of police officers and members of the Special Constabulary has been extended to include persons applying for police staff vacancies.

4. Process

4.1 Individuals requiring a CTC, SC or DV security clearance must complete the appropriate security questionnaire(s) only after the appropriate RV or MV checks have been satisfactorily completed. In this way, individuals are not entering the NSV process until actually required to do so. If this is impracticable and individuals are required to complete the Security Questionnaire(s) at the same time as the Force Vetting questionnaire(s), they must be advised that processing of the Security Questionnaire(s) and, therefore, consideration of NSV is conditional on RV, MV or EMV being granted.

4.2 Vetting enquiries should be conducted in respect of all individuals named on the vetting questionnaires who are over the age of criminal responsibility i.e. 10 years in England and Wales, 8 years in Scotland.

4.3 The following checks are suggested as a minimum for RV:

- Police National Computer (PNC)/ Criminal History System (CHS) / Crime Information System (CIS) check on the applicant, partner, partner's parents, close family members, associates and any other person residing with the applicant for convictions, cautions and other outstanding matters (Taint must also be considered. See paragraph 5.3 below);
- Police intelligence check on the applicant, family members/associates and their addresses;
- Special Branch checks;
- Impact Nominal Index (INI) check (where available);
- Other Force Checks on the applicant and family members/associates and last five years of applicants' address(es);
- Record Management System check (historical hard copy records, where available) on the applicant;
- Crime Report Allegations;
- Voters Records check;
- Check of Vetting Database;
- Credit reference check;
- Internet (open source) enquiries (if felt appropriate);
- A Professional Standards Check should also be considered where necessary (through previous service or employment);
- MOD Check where applicable

4.4 In all cases clearance must be processed and a decision reached as soon as reasonably practicable.

5. Convictions, Cautions and Other Relevant Matters and Judicial Disposals

5.1 A check is to be made of PNC/CHS/CIS records for any cautions and/or convictions recorded against the applicant, partner, partner's parents, close family members, associates and any other person residing with the applicant,. Applicants who fail to declare a relevant matter, including any convictions, cautions and judicial or other formal disposals, whether spent or not, should be refused clearance at this stage on the grounds of integrity.

5.2 Applicants with convictions, cautions and judicial or other formal disposals recorded may be granted vetting clearance in accordance with the Convictions and Cautions SOP 8. The vetting decision on applicants with impending prosecutions and current investigations should be deferred until the outcome is known.

5.3 In applying the eligibility criteria set out in SOP 8, due regard needs to be given to the appointment of police personnel who may be required to give evidence in judicial proceedings. It is essential that they are carefully screened to ensure that they are not likely, because of any previous convictions, cautions and judicial or other formal disposals, to be restricted in their ability to act as 'witnesses of truth'. On considering convictions, cautions and judicial or other formal disposals all aspects of Chapter 18 of the CPS Prosecution Team Disclosure Manual must be taken into account. (See SOP 17)

5.4 Difficulties can occur when individuals with previous convictions, cautions, judicial or other formal disposals have received recruitment vetting clearance and subsequently apply for a role requiring greater involvement in the evidential chain.

5.5 The impact of appointing a police officer or member of police staff who is, or can be, within the evidential chain and who is effectively 'tainted' cannot be underestimated and can heavily affect the deployment of such an officer or member of police staff on appointment, and in some cases throughout their career. Generally the impact of 'taint' will lessen as the time since the 'finding' recedes. Thus when allowing a 'tainted' individual to become a police officer or fulfil any other role which will involve them being placed in the evidential chain, they must be made aware of the impact that such a requirement will have on their career. Particular care must therefore be taken when clearing an applicant who will have to disclose;

- criminal convictions, criminal cautions and penalty notices;
- other judicial disposals;
- criminal proceedings which have not been completed;
- adverse judicial findings;
- police discipline;
- disciplinary findings of guilt at a misconduct tribunal;
- relevant formal written warnings and relevant disciplinary cautions;
- disciplinary proceedings which have not been completed.

5.6 Further guidance can be obtained from the CPS Prosecution Team Disclosure Manual.

6. Police Intelligence Records

6.1 Intelligence/information records and other non-conviction databases must be searched for the name of the applicant and any current or previous home address(es) provided at which the applicant has resided in the last five years. Such checks should also be

conducted in respect of the current home address of all other individuals named on the vetting questionnaires or others who come to notice during the vetting process.

6.2 Should these checks reveal any intelligence or information held surrounding the applicant and family members and their home addresses, this data will be classified and assessed using the 5x5x5 intelligence assessment system.

6.3 Where a police officer, member of the special constabulary or member of police staff is required to resign, dismissed or resigns in anticipation of misconduct proceedings, a flagstone marker should be created on the force intelligence system to ensure that the existence of intelligence will be detected as a result of an IMPACT Nominal Index (INI) check.

7. Other Force Intelligence/Information (LIO) Check

7.1 'Other Force' intelligence checks should be conducted on the applicant and others as above, who live outside the home force area. Checks should be made in the policing area where the applicant currently resides and all policing areas where the applicant has resided any time in the last five years, as detailed in SOP 13.

7.2 The INI should be used to achieve this purpose. However, where this has not be made available for vetting purposes and where an applicant has resided outside the force area the individual is being cleared to work within, that force should contact the force area where the individual has resided, at any time, in the last five years.

7.3 Where access to INI has been granted searches using INI should be conducted against the applicant and any other individual named on the vetting documentation or, where information has given rise to the need to expand the search, any other individual discovered during vetting enquiries. The search should be undertaken using the 'find nominal' field.

7.4 Any positive 'traces' must be followed up with a formal request to the relevant Force Vetting Unit (regardless of whether that force area was identified on the applicant's documentation) giving relevant details of the trace obtained via INI along with the core details of name, date and place of birth, to facilitate the further search. It is recommended that the relevant record held on INI should be transferred into a 'PDF' or 'word' document and forwarded to the force(s) which holds the information requested.

7.5 All non-conviction material and/or information and/or intelligence to be revealed should be returned to the Force Vetting Unit who made the request. It is the responsibility of the requesting force to decide upon the relevance of the information. All material provided must be treated in accordance with the Data Protection Act and the 5x5x5 intelligence grading restrictions (for DPA purposes the force responding to the request remains the Data Controller and therefore, retains legal responsibility for any breaches of DPA relating to any further distribution or disclosure of material provided and therefore, 5x5x5 restrictions must be made clear to the receiving force).

7.6 All forces should respond to the request for information within the ACPO National Vetting Working Group (NVWG) Service Level Agreement of 14 calendar days. The response, and request, should be through the preferred option of secure e-mail.

8. Records Management Check

8.1 Details of the applicant, partner, partner's parents, close family members, associates and any other person residing with the applicant will be checked against historical

investigation files. Generally speaking, there is no need to call for a file when the applicant is shown as the victim of a crime. However, in all other cases it is recommended that the file be reviewed.

9. Crime Report Information System

9.1 Details of the applicant, partner, partner's parents, close family members, associates and any other person residing with the applicant should be checked against the suspect and accused records. The applicant's address should also be checked. Searching the applicant's address will identify allegations of crime affecting other persons residing with the applicant.

10. Professional Standards Check

10.1 Where any previous police service, either as a police officer, member of police staff or special constable, has been indicated or ascertained, details of such applicants for appointment as police officers, members of the Special Constabulary and police staff, should be forwarded to Professional Standards Departments for checking against Professional Standards complaints, misconduct and intelligence databases as part of the RV process.

10.2 The check should be carried out with the force the applicant worked for or was deployed with as well as the force the applicant has applied for.

11. Voters check

11.1 Details of the applicants address must be checked against the voters register. Applicants who are not shown on the register must have their previous address checked. If the applicant is not shown on the voter's register, they must be contacted to establish further information. Additional identity checks must be considered for applicants not shown on the voter's register.

12. Check of security files

12.1 Vetting Databases must be checked to establish if the applicant has ever held security clearance with the home force in the past and if there were any security breaches or incidents relating to that clearance period.

13. Credit Reference Checks

13.1 The financial questions incorporated in the Home Office application form for Police Officers should be used in the recruitment of Police Staff. The information provided in the questionnaire should be compared with the results of a credit reference check.

13.2 A credit reference check should be carried out to ascertain the financial status of the applicant and cross-referenced against the information provided by the applicant. Certain financial issues should result in rejection. Further information is given in Financial Checks SOP 18 and NPIA Circular 01/2010.

14. Interviewing of applicants

14.1 Applicants should be interviewed where necessary in order to clarify queries, ambiguities or concerns raised during the vetting process. Further guidance is available in SOP 7.

15. Referees

15.1 The role of checking against references is one which falls to the recruiting authority/Unit and is completed as part of the recruitment function. Discretion should be exercised and used when deciding whether to ask for personal referees. As a general rule, personal referees should only be used in difficult cases or where concerns are raised during the vetting process.

16. Review of checks and enquiries

16.1 At this stage the vetting officer should review the results of all enquiries and checks carried out. A report outlining all adverse traces and other relevant information arising from the vetting enquiries should be passed to the vetting decision maker.

16.2 Great care should be taken when considering information revealed as part of the vetting process which relates to an individual's mental or physical health which would tend to indicate a vulnerability which could result in the applicant being unsuitable for appointment by the force. Neither police officers nor Force Vetting Officers (FVOs) are qualified to make such assessments of medical conditions or mental health. Therefore, any medical information, such as intelligence reports or allegations etc., revealed as part of the vetting process must be passed to the Force Medical Officer (FMO) or Occupational Health Unit for a full, professional assessment to be made.

16.3 Following such an assessment the FMO or Occupational Health Unit will decide if the applicant is suitable for appointment by the force. Under no circumstances should any medical information be passed to Force Vetting Units.

17. The clearance decision

17.1 The decision maker, usually the FVO, should review the case and make a decision as to whether to grant clearance or not. However, before making a final decision the decision maker may ask for additional checks or enquiries to be made, for example calling the applicant in for an interview or asking for personal referees.

17.2 The front of the vetting file should be stamped 'No Vetting Objection" (NVO) or REFUSED according to the vetting decision.

17.3 All vetting decisions must be fully documented with the rationale for the decision. Difficult or complicated cases should be passed to the next level of vetting unit management for advice.

17.4 Due to the length of the recruitment process, some individuals are not appointed for several months after their application is received. Because of this delay, the information provided in the application forms could be out of date. Cases have occurred where individuals have been arrested or convicted of criminal offences during the interim period, or have accrued debts, or experienced other changes in their lifestyle that could have precluded them from being appointed. Some applicants have also failed to provide accurate details as to family members, criminal associates, finances or other relevant information. When these omissions are subsequently discovered they have resulted in disciplinary procedures being instigated, or individuals being considered for discharge under Police Regulations or Police Staff Standards of Professional Behaviour.

17.5 Forces are therefore recommended to provide a briefing to all Police Officer Recruits before attestation, providing them with their original application forms and security questionnaires, and stressing the requirement for the provision of accurate information.

They should be warned of the consequences of their failure to do so, and required to either re-sign and re-date their application forms and security questionnaires, or sign a separate declaration giving them the opportunity to declare any involvement with the police, other law enforcement agencies or statutory prosecuting authority. Where applicants notify relevant changes, the implications of their declarations should be assessed prior to attestation. Whilst the Home Office has indicated that legally this process is not required it is good practice to do so, as it will prevent the recruitment of inappropriate applicants, reduce the need for misconduct hearings and limit the number of legal challenges.

17.6 The requirement for accurate and up to date vetting information applies equally to Members of the Special Constabulary and Police Staff.

18. Review

18.1 Applicants for recruitment to the police community have no right of appeal against a decision not to offer them appointment, based on the vetting outcome. However, it is suggested, as best practice, that a review procedure is made available (see SOP 9).

19. Periodic Review

19.1 An annual, or other specified periodic, review should take place using the appropriate *Security Appraisal Form*. Any clearance may be reviewed at an earlier stage, or prior to the review date, if adverse information comes to light relating to the subject's clearance, or a material change in an individual's personal circumstances.

19.2 On appointment, individuals should be informed that adverse changes in circumstances, or failure to notify such changes, could result in the withdrawal of their vetting clearance and/or the initiation of misconduct proceedings.

20. Renewal of vetting clearance

20.1 RV clearances must be renewed every ten years. However, clearance may be renewed at an earlier stage, according to the relevant Force Policy, or if adverse information comes to light relating to the subject's clearance, or there is a material change in individual's personal circumstances.

21. Forms

21.1 Attached are suggested forms that can be adapted for each force, for use where standard national forms are not already available. However the captions and details required should be adopted by forces as a national minimum standard.

22. Responsibilities

22.1 This SOP is owned by the ACPO Professional Standards Committee.

22.2 Responsibility for implementing and reviewing the SOP rests with the ACPO National Vetting Working Group.

23. Associated Documents and Policies

- ACPO / ACPOS National Vetting Policy for the Police Community
- Manual of Protective Security

- Crown Prosecution Service (CPS) Prosecution Team Disclosure Manual
- NPIA Circular 01/2010
- Authentication SOP 2
- Vetting Interviews SOP 7
- Convictions and Cautions Criteria SOP 8
- Appeals and Reviews SOP 9
- Other Force Vetting Checks SOP 13
- Adverse Information and Judicial Findings (TAINT) SOP 17
- Financial Checks SOP 18

ACPO Professional Standards Committee

Standard Operating Procedure Number 4

MANAGEMENT VETTING and ENHANCED MANAGEMENT VETTING

Protective Marking	NOT PROTECTIVELY MARKED
Publication Scheme Y/N	Yes
Title	Management Vetting and Enhanced Management Vetting
Version	3.0
Summary	This Standard Operating Procedure supports the ACPO / ACPOS National Vetting Policy for the Police Community
Enhanced	ACPO National Vetting Working Group
Author	Carol Benton [Lancashire], Stewart Finlayson [Strathclyde], Jonathan Gupta [Staffordshire], Bob Lane [Warwickshire], Alan McCawley [MPS]
Date created	August 2010
Review date	August 2011

1. Introduction

1.1 This Standard Operating Procedure (SOP) supports the ACPO/ACPOS National Vetting Policy for the Police Community (NVP) and associated documents and policies.

1.2 This is a new SOP.

2. Application

2.1 This SOP comes into force on 1st August 2010.

3. Purpose

3.1 The purpose of 'Management Vetting (MV) and Enhanced Management Vetting' (EMV) is to provide a means of ensuring that persons serving in 'designated posts', which are those with access to sensitive police premises, information, intelligence, financial or operational assets, have been assessed as to their reliability and integrity. The procedure therefore serves to reduce the risks of unauthorised disclosure, or loss of, sensitive police assets.

3.2 It is recommended that all persons with long term, frequent and uncontrolled access to SECRET – POLICE, and occasional access to TOP SECRET – POLICE assets, should hold MV clearance. Those who require regular and uncontrolled access to TOP SECRET – POLICE assets should hold EMV clearance. The EMV procedure has been developed to formalise the recommendation made in Version 1 of this policy that additional checks should be added to the MV procedure to counter specific threats.

3.3 However, MV and EMV clearances are a requirement for service in all 'designated posts', irrespective of whether post-holders have access to police or government protectively marked assets. e.g. those awarding contracts or handling sensitive financial assets. For individuals entering directly into a designated post, the RV process should be completed first, supplemented by the MV or EMV process once the RV decision has been made.

3.4 As MV and EMV clearances are a pre-requisite of appointment to 'designated' posts, individuals who refuse to undertake the procedure will not be considered for appointment.

3.5 Individuals already in post will be encouraged to take part in the process but, if they refuse or fail the vetting process, line managers, together with the Force Vetting Officer (FVO), will need to assess the risk and decide whether it is practical to 'manage' them in the workplace, if necessary, by preventing their access to sensitive material. Police officers who refuse to undergo the procedure and cannot be 'managed' in post must be transferred to other duties. However, for police staff contractual conditions may make their redeployment more difficult and may, in the most extreme cases, require termination of their contract. This decision would only be made at the appropriate ACPO/ACPOS level and following consultation with Human Resources and the relevant staff association or recognised Trade Union.
NB: Termination of an individual's services through the aforementioned process does not in any way impinge on their right to appeal against dismissal through the appropriate channels.

3.6 Existing police officers and members of police staff will be permitted to remain in 'designated posts' whilst the vetting procedure is carried out. New appointees should not be appointed until after vetting clearance has been granted.

3.7 In relation to National Security Vetting (NSV), MV is a prerequisite to Security Check (SC) and Developed Vetting (DV) clearance. This is due to the fact that the checks undertaken for NSV clearance in terms of criminality are not sufficiently thorough for the purposes of the police community.

3.8 To maintain the integrity of the separate SC, DV, MV procedures, all MV enquiries must be completed, and MV clearance granted, prior to making the SC or DV clearance decision. In practice, this means that most of the requirements of the SC or DV procedure will have been carried out under the MV or EMV process.

3.9 However, it should be noted that there will be posts which require MV or EMV clearance, but which do not require NSV clearance.

3.10 Where elements of the SC or DV are completed as part of the MV or EMV the enquiries do not need to be duplicated.

4. Process

4.1 Forces should conduct an audit of all posts and designate the relevant level of vetting to each post. In designating levels of vetting, in addition to access to protectively marked material and the criteria outlined in 3.1 above, consideration should also be given to other relevant factors, including but not limited to;

- The impact of corruption, or disclosure of information, or intelligence, or whether actions can lead to significant harm, or
- loss to the organisation, or
- harm or loss to an individual, or
- Loss of life.

4.2 The MV and EMV processes rely on the completion of personal information and financial questionnaires providing relevant information, and written authorisation, for the following checks and associated enquiries to be carried out, as a suggested minimum;

MV:

- Proof of identity (if required);
- Proof of residence (if required);
- CHS / PNC / CIS;
- Local Intelligence Databases;
- INI;
- Other Force Checks (where INI is not used);
- All Force Databases (including non-conviction databases);
- Special Branch;
- MOD (where relevant);
- Professional Standards complaints and misconduct and intelligence databases;
- Personal finances (includes financial questionnaire, force credit reference check and assessment of information returned);
- Liaison with Occupational Health (where required);
- Internet (open source i.e. search engines and Social Networking sites);

- Enquiries relating to vulnerability to pressure or inducements (includes the indiscriminate use of alcohol or drugs and/or gambling);
- References from current and / or former supervisors to cover a minimum 12 month period;
- Interviews with current and former supervisors to be conducted at the discretion of the FVO;
- Interviews with the person subject to the vetting procedure to be conducted at the discretion of the FVO.

EMV:

As above, plus a suggested minimum of:

- Enhanced financial questionnaire;
- Credit reference check on spouse or partner (where applicable - consent **must** be provided for this by spouse / partner);
- Mandatory interviews with persons subject of the vetting procedure;
- Personnel files;
- Peer references;
- Medical assessment by Force Medical Officer (FMO);
- References;
- Enquiries and interviews with current and former supervisors.

4.3 Attached as Appendix 1 and Appendix 2 are sample MV and EMV questionnaires. These are not mandatory, but it is suggested that the information captured by these forms will satisfy the requirements of an MV or EMV as relevant.

4.4 The purpose of financial checks is to assess whether applicants are, or have been, in serious financial difficulty or show signs of financial irresponsibility to the extent they could become vulnerable to financial inducement. The financial scoring system used is based on the Cabinet Office system for NSV. The assessment form allows comparison between the information contained in the financial questionnaire and that provided by the credit reference check.

4.5 The financial questionnaire seeks to gather information in the following seven areas:

- Indications of previous financial unreliability;
- Problems meeting current commitments;
- Indications of poor financial judgement;
- Potential for future financial difficulties;
- Assets possibly inconsistent with income;
- Potential conflict of interests;
- Business interests.

5. Factors which may create a presumption of unfitness

5.1 The following factors may, through dishonesty or lack of integrity, create a presumption of unfitness for appointment to 'designated posts':

- Past infringement of security or vetting policy or procedures;
- Significant or repeated breaches of discipline;
- Providing false or deliberately misleading information, or omitting significant information from the vetting questionnaires;
- Unauthorised association with persons with previous convictions or reasonably suspected of being involved in crime;

- Criminal convictions or cautions.

6. Circumstances which may impair judgement

6.1 The following circumstances are regarded as likely to impair judgement or may result in vulnerability to pressure or inducements:

- Significant financial difficulties or debts;
- Misuse of alcohol;
- Gambling;
- Misuse of controlled or prescribed drugs;
- When the FMO certifies that appointment to such posts could present a risk to the confidentiality, integrity or availability of intelligence assets (in these circumstances the FMO will advise the post holders to notify their immediate or senior supervisors, and will notify the FVO of his decision).

7. Assessing the criteria for trustworthiness

7.1 In making an assessment as to whether or not to grant MV or EMV clearances the following matters will be taken into consideration:

- The security implications of any adverse information obtained during the vetting process (for example it may be necessary to give greater weight to some factors than to others);
- A careful assessment of the significance of any past conduct or circumstances;
- Distinctions will be drawn between isolated or minor blemishes on an individual's record and information pointing to habitual or significant vulnerabilities.

8. Assessment of Information

8.1 Great care should be taken when considering information revealed as part of the vetting process which relates to medical issues. Neither police officers nor FVOs are qualified to make such an assessment of medical conditions or mental health. Therefore, any medical information such as intelligence reports or allegations etc. revealed as part of the vetting process, must be passed to the FMO or Occupational Health Unit for a full professional assessment to be made.

8.2 Following such an assessment the FMO or Occupational Health Unit will decide if the applicant is suitable for appointment within the force. Under no circumstances should any medical information be passed to Force Vetting Units.

9. Following a decision to grant clearance

9.1 The FVO will ensure that, in cases where clearance is granted, any reservations or limitations are clearly recorded and clearances notified in writing to Divisional Commanders and Heads of Departments responsible for the position the individual is moving to. The subject should be made aware that any limitations will be notified to their line management.

9.2 In notifying individuals that vetting clearance has been granted they will be reminded of their responsibilities for protecting both force and National Security assets and of the requirements of the Data Protection Act, Official Secrets Acts, Computer Misuse Act and force security policies and procedures. They should also be reminded of the obligation placed on them to notify any significant changes in their personal and financial circumstances.

9.3 If clearance is refused, or there are any limitations to the clearance, individuals will be informed and, where possible, provided with an explanation. However, there may be circumstances, for example in cases where notification could prejudice a criminal or disciplinary inquiry, or when disclosure would breach the Data Protection Act or other legislation, where information may be withheld. In addition, information may have been provided by third parties, in confidence, during vetting enquiries. Such information will only be disclosed to the subject if the person who has provided the information agrees to its disclosure. Because of a lack of relevant background information, temporary staff, those on work experience, or persons under 17 years of age, will not be employed in departments or units which include 'designated posts', without the authority of the FVO.

10. Appeals

10.1 If an internal applicant disputes the decision to refuse, withdraw or suspend MV or EMV clearance, an internal appeal can be made, as detailed in SOP 9.

11. Reviews

11.1 External applicants for recruitment to the police community have no right of appeal against a decision not to offer them appointment, based on the vetting outcome. However, it is suggested as best practice that a review procedure is made available. There is no right to a personal hearing.

11.2 A letter requesting a review should be forwarded to the nominated officer within 14 days of receipt of written notification of the decision. The review will be conducted by a nominated individual who has not been involved in the original decision, and will then review the original decision within 28 days of receipt of the letter of review and provide the applicant with a written statement outlining the result of the review. The decision reached will be final. There is no right to personal representation at a review.

12. Aftercare

12.1 MV and EMV clearances should be renewed every 5 years. However, any clearance may be reviewed at an earlier stage if adverse information comes to light relating to the subject, or there is a material change in an individual's personal circumstances. In addition, all MV and EMV clearances should be the subject of a formal annual security review involving line management.

12.2 Changes in the personal circumstances of individuals holding MV and EMV clearances may impact upon their continued suitability to hold that clearance. They must therefore report any relevant changes, including spouses, partners or civil partners, changes of address, criminal associations, or other matters relating to the risk factors outlined above, in writing, to the FVO. It is also the responsibility of line managers to ensure that the FVO is notified of relevant changes coming to their attention.

12.3 At the time of clearance post holders should be informed that failure to notify relevant changes could result in the withdrawal of their vetting clearance. However, individuals should be aware they can report any changes in the knowledge that notifications will be met with a sympathetic response, and that it would only be in the most serious cases that consideration would be given to the withdrawal of clearance.

12.4 Individuals with MV or EMV clearances who transfer to a 'non-designated' post will retain their vetting clearance for up to 12 months from the date of transfer from the designated post. At that time the clearance will lapse. Annual security reviews and aftercare will no longer apply after individuals leave an MV or EMV post. If they transfer back to an MV or EMV post within 12 months of leaving, their MV or EMV clearance will remain valid until the renewal period, subject to an annual security review.

12.5 If an individual with MV or EMV clearance transfers to another force or agency, the vetting status will remain valid until the renewal date, subject to the satisfactory completion of an annual security review form, for the information of the receiving force. The receiving force retains the right to require an individual to complete the full MV or EMV process.

13. Responsibilities

13.1 This SOP is owned by the ACPO Professional Standards Committee.

13.2 Responsibility for implementing and reviewing the SOP rests with the ACPO National Vetting Working Group.

14. Associated Documents and Policies

- ACPO / ACPOS National Vetting Policy for the Police Community
- Security Policy Framework (SPF)
- Appeals/Review Procedure SOP 9

ACPO Professional Standards Committee

Standard Operating Procedure Number 5

NON POLICE PERSONNEL VETTING (NPPV)

Protective Marking	NOT PROTECTIVELY MARKED
Publication Scheme Y/N	Yes
Title	Non Police Personnel Vetting
Version	3.0
Summary	This Standard Operating Procedure supports the ACPO / ACPOS National Vetting Policy for the Police Community
Management	ACPO National Vetting Working Group
Author	Carol Benton [Lancashire], Stewart Finlayson [Strathclyde], Jonathan Gupta [Staffordshire], Bob Lane [Warwickshire], Alan McCawley [MPS]
Date created	August 2010
Review date	August 2011

1. Introduction

1.1 This Standard Operating Procedure (SOP) supports the ACPO/ACPOS National Vetting Policy for the Police Community (NVP) and associated documents and policies.

1.2 This is a new SOP.

2 Application

2.1 This SOP comes into force on 1st August 2010.

3. Purpose

3.1 The purpose of 'Non Police Personnel Vetting' (NPPV) is to provide a means of ensuring that any persons other than police officers, police staff and members of the Special Constabulary, having physical or remote access to police premises, information, intelligence, financial or operational assets have been assessed as to their reliability and integrity and thus suitability for clearance. The procedure serves to reduce the risks of unauthorised disclosure or loss of sensitive police assets.

3.2 NPPV relates to the vetting of individuals other than police officers, police staff and members of the Special Constabulary who require access to police premises without constant supervision, and/or police information, corporate databases, data networks or hard copy material, either through direct or remote access. These include, but are not limited to, statutory crime and disorder partners, HM Revenue and Customs, UK Borders Agency, third party agents, Police Authority staff and members depending on role, and a variety of contractors and volunteers, consultants, auditors and researchers.

3.3 If a non-police person declines or refuses to be vetted, their access to police assets will be restricted, along with those described in 3.4 below.

3.4 Non-police personnel, who are admitted to police premises but who are accompanied or remain under constant supervision and are not permitted access to police information systems or protectively marked material, need not be vetted. In these circumstances, existing procedures for the reception of visitors should apply.

3.5 In relation to the multifarious group of people to which NPPV applies, careful consideration should be given to the level of NPPV to be applied to each role, taking into consideration the information, intelligence and other assets, to which the individual will have access. This is to ensure that non-police personnel are not subject to a disproportionate level of vetting.

4. Process

4.1 There are three NPPV Levels, as follows; NPPV 1, NPPV 2 and NPPV 3.

4.2 The authentication procedure (SOP 2) must be completed prior to NPPV being initiated. Authentication on its own does not allow access to police protectively marked assets, or unescorted access to any police premises.

4.3 Non-police personnel who require long-term frequent and uncontrolled access to SECRET government assets require NPPV Level 3 clearance, supplemented by an SC check.

4.4 NPPV relies on the provision of personal information and, where relevant, financial details, and written authorisation for the appropriate checks and associated enquiries to be carried out. The purpose of financial checks is to assess whether applicants are, or have been, in serious

financial difficulty, or show signs of financial irresponsibility to the extent they could become vulnerable to financial inducement.

5. Level 1. Limited Access – No Protectively Marked Assets

5.1 Level 1 applies to those persons having unsupervised access to police premises on an ad hoc and irregular basis but no access to any electronic systems and/or hard copy material. In the main this applies to utility workers such as plumbers, electricians etc and may, on occasions, apply to individuals on work experience etc if they have NO access to protectively marked information or electronic systems.

5.2 This level does not afford any access to protectively marked police material or assets.

5.3 ***Minimum Standard Requirement:*** PNC/CHS/CIS and INI/local intelligence and other non-conviction databases, including Special Branch on applicant only

5.4 **Length of clearance:** 12 months

6. Level 2. Unsupervised Access – Protectively Marked Assets up to CONFIDENTIAL

6.1 Level 2 applies to those persons having frequent and regular unsupervised access to police premises and/or access to police information and/or hard copy material or protectively marked material, either on police premises or by remote access.

6.2 Level 2, supported by authentication, allows regular access to police protectively marked assets up to CONFIDENTIAL and occasional access up to SECRET.

6.3 It is the responsibility of the employer to ensure that the authentication process is completed and that references are sought.

6.4 ***Minimum Standard Requirement***: PNC/CHS/CIS and INI/local intelligence checks, other non-conviction databases and Special Branch for applicant, spouse/partner and co-residents. Military and Professional Standards checks on the applicant if required. Credit Reference check on applicant. CTC may be applied where appropriate.

6.5 **Length of Clearance**: 3 years

7. Level 3. Unsupervised Access – Protectively marked Assets up to SECRET

7.1 Level 3 applies to all Non Police Personnel who require long term, frequent and uncontrolled access to SECRET – POLICE, and occasional access to TOP SECRET – POLICE assets.

7.2 Level 3, supported by an SC, allows long-term frequent and uncontrolled access up to SECRET government assets.

7.3 ***Minimum Standard Requirement:*** Checks as required for Level 2 clearance to be conducted on applicant and all family members and co-residents, with full financial checks on the applicant which may be supplemented by CTC or an SC. Also requires annual security review.

7.4 **Length of Clearance:** 5 years, with annual security review.

8. National Police Systems Contractors

8.1 This is a national process for **National Police System Contractors** as follows:

8.2 Warwickshire Police currently on behalf of all police forces in England, Wales, Scotland and Northern Ireland, have agreed to vet all National Police System Contractors to a level appropriate to the requirements of the ACPO / ACPOS NVP, and to act as an authority in that respect.

8.3 This system will eradicate the need for forces to vet and re-vet individual contractors and will be at no cost to forces.

8.4 The level of vetting will be as per NPPV Level 3.

8.5 ***Minimum Standard Requirement:*** As Level 3.

8.6 **Length of clearance:** 5 years with annual security review

9. Checkable History

9.1 The authentication procedure (SOP 2) must be completed prior to NPPV being initiated. At present satisfactory Force Vetting checks abroad cannot be achieved. It is essential that vetting criteria applies to all applicants, thus when such checks can be carried out to the same extent that they are in the UK then residency criteria would not be a bar to recruitment. The rationale behind the residency criteria / checkable history is given in SOP 2, together with a description of the provisions relating to the permissible departure from this, in exceptional circumstances.

10. Appeals / Reviews

10.1 Applicants for NPPV have no right of appeal against a decision not to grant the relevant level of clearance. However, it is suggested as best practice that a review procedure is made available, as detailed in SOP 9.

11. Aftercare

11.1 Tenure of clearances will vary subject to a number of factors. Levels 1 and 2 will not require aftercare but Level 3 will.

11.2 For Level 3 an annual security review should take place using the appropriate form.

11.3 Any clearance may be reviewed at an earlier stage, or prior to the review date, if adverse information comes to light relating to the subject, or there is a material change in an individual's personal circumstances.

11.4 Changes in the personal circumstances of individuals holding NPPV clearance may impact upon their continued suitability to hold that clearance. They must, therefore, report any relevant changes, including spouses or partners, changes of address, criminal associations, or other matters relating to the risk factors outlined above in writing, to the Force Vetting Officer.

11.5 Individuals should be informed that adverse changes in circumstances, or failure to notify such changes, could result in the withdrawal of their vetting clearance.

12. Forms

12.1 Attached are suggested forms that can be adapted for each force. However the captions and details required should be adopted by forces as a national minimum standard.

13. Responsibilities

13.1 This SOP is owned by the ACPO Professional Standards Committee.

13.2 Responsibility for implementing and reviewing the SOP rests with the ACPO National Vetting Working Group.

14. Associated Documents and Policies

- ACPO / ACPOS National Vetting Policy for the Police Community
- Security Policy Framework (SPF)
- Authentication SOP 2
- Appeals/Review Procedure SOP 9
- Aftercare SOP10
- Risk Assessments – Third Party SOP 17

ACPO Professional Standards Committee

Standard Operation Procedure Number 6
National Security Vetting

Protective Marking	NOT PROTECTIVELY MARKED
Publication Scheme Y/N	Yes
Title	National Security Vetting
Version	3.0
Summary	This Standard Operating Procedure supports the ACPO / ACPOS National Vetting Policy for the Police Community
Management	ACPO National Vetting Working Group
Author	Carol Benton [Lancashire], Stewart Finlayson [Strathclyde], Jonathan Gupta [Staffordshire], Bob Lane [Warwickshire], Alan McCawley [MPS]
Date created	August 2010
Review date	August 2011

1. Introduction

1.1 This Standard Operating Procedure (SOP) supports the ACPO/ACPOS National Vetting Policy for the Police Community (NVP) and associated documents and policies.

1.2 This is a new SOP.

2. Application

2.1 This SOP comes into force on 1st August 2010.

2.2 The Authentication procedure (SOP 2) and Recruitment Vetting (RV) (SOP 3) must be completed prior to any level of National Security Vetting (NSV) being initiated. Additionally, Management Vetting (MV) (SOP 4) must be completed before a Security Check (SC) or a Developed Vetting check (DV) is initiated.

3. Purpose

3.1 The purpose of HMG's personnel security controls (including NSV) is to provide a level of assurance as to the trustworthiness, integrity and reliability of all HMG employees, contractors and temporary staff who, in the course of their work, have access to, or knowledge or custody of, sensitive government assets which carry a 'PROTECT', 'RESTRICTED', 'CONFIDENTIAL', 'SECRET' or 'TOP SECRET' protective marking, under the Government Protective Marking Scheme (GPMS), or those who satisfy the requirements for Counter Terrorist Check (CTC), as outlined in paragraph 6.1 below.

3.2 There are four levels of personnel security controls available depending on the level of assurance required:

- Baseline Personnel Security Standard (BPSS)
- Counter Terrorist Check (CTC)
- Security Check (SC)
- Developed Vetting (DV)

Of these, CTC, SC and DV are all formal security clearances obtained through the NSV process. The BPSS is not a formal security clearance, but it underpins the NSV process and its satisfactory completion is a prerequisite for CTC, SC and DV.

3.3 Details of HMG's policy on personnel security are contained in the Cabinet Office Security Policy Framework (SPF). In the context of NSV, police forces are regarded as 'agencies'.

4. Personnel Security Risk Assessment

4.1 Security risk assessments deliver a range of benefits to organisations, from ensuring that counter-measures are cost-effective to fostering a shared understanding of security priorities. The Centre for the Protection of National Infrastructure (CPNI) has developed good practice guidance on risk assessment for personnel security and organisations applying HMG's personnel security policy are required to ensure that they adopt such a risk management approach to their personnel security arrangements.

5. HMG Baseline Personnel Security Standard (BPSS)

5.1 The BPSS is the recognised standard for HMG pre-employment screening. It forms the foundation of NSV and seeks to address identity fraud, illegal working and deception generally. It comprises verification of four main elements: identity; employment history (past three years); nationality and immigration status (including the right to work); and, if a formal NSV clearance is not required for the post, unspent criminal records. In addition, prospective appointees are required to account for any significant periods (six months or more in the past three years) of time spent abroad.

5.2 Satisfactory completion of the BPSS allows regular access to government assets marked up to CONFIDENTIAL and occasional access to government assets marked SECRET, provided an individual has a need to know.

5.3 The BPSS applies to all civil servants, members of the armed forces, temporary staff and government contractors generally. Police forces are not required to apply the BPSS itself; application of the Authentication procedures (SOP 2) plus either Recruitment Vetting (RV) (SOP 3), or NPPV levels 2 or 3 (SOP 5) fully meets the requirements of the BPSS.

6. Counter Terrorist Check (CTC)

6.1 A CTC clearance is required for those individuals who are to be appointed to posts which:

- involve proximity to public figures who are assessed to be at particular risk from terrorist attack;
- give access to information or material assessed to be of value to terrorists;
- involve unescorted access to certain military, civil, industrial or commercial establishments assessed to be at risk from terrorist attack.

6.2 For the police, this means that only police officers, members of the Special Constabulary, police staff (including Force Support Officers) and non-police personnel whose work involves access as described above require CTC clearance. Individuals serving in SC and DV designated posts will be CTC cleared as part of those processes.

6.3 It is not intended that all police officers and police staff should be CTC cleared as a matter of course. However, it is important that individual forces assess all posts within their force and identify those which fall within the criteria in 6.1 and subject only these to CTC clearance. The decision as to whether a CTC is required for an individual is a matter for the Chief Officer.

7. Security Check (SC)

7.1 An SC clearance is required for those individuals who are to be appointed to posts which:

- require long term, frequent and uncontrolled access to government assets marked SECRET;
- require occasional, supervised access to government assets marked TOP SECRET (such as Chief Constable's Staff Officer and those in Special Branch);

and for individuals who:

- while not in such posts, will be in a position to directly or indirectly bring about the same degree of damage;
- will have sufficient knowledge to obtain a comprehensive picture of a SECRET plan, policy or project;
- are being considered for appointment where it would not be possible to make reasonable career progress without security clearance for access to government assets marked SECRET;
- need access to certain levels of protectively marked material originating from another country or international organisation.

7.2 An SC clearance should not normally be required for:

- occasional access to government assets marked SECRET in the normal course of business or during conferences, briefings or courses;
- custody of a small quantity of government assets marked SECRET;
- entry to an area where government assets marked SECRET are stored;
- work in areas where government information at SECRET and TOP SECRET might be overheard;
- use of equipment capable of handling government information marked SECRET, provided that access controls are in place.

In the above circumstances, the BPSS, or Authentication supported by RV or NPPV level 2 or 3 should usually be sufficient.

7.3 Where an SC clearance is required for access to SECRET STRAP material, a review of personal finances must be carried out. This is referred to as an SC (Enhanced) clearance.

8. Developed Vetting (DV)

8.1 A DV clearance is required for those individuals who are to be appointed to posts which:

- require frequent, uncontrolled access to government assets marked TOP SECRET or require any access to TOP SECRET STRAP, ATOMIC or other codeword material;

and for individuals who:

- while not in such posts, will be in a position to directly or indirectly bring about the same degree of damage;
- require frequent, uncontrolled access to Category I nuclear material;
- need access to certain levels of protectively marked material originating from another country or international organisation.

8.2 A DV clearance should not normally be required for:

- occasional, supervised access to limited quantities of government assets marked TOP SECRET in the normal course of business or during conferences, briefings or courses;
- custody of a small quantity of government assets marked TOP SECRET;
- entry to an area where government assets marked TOP SECRET are stored;

- work in areas where government information at TOP SECRET might be overheard;
- use of equipment capable of handling government information marked TOP SECRET, provided that access controls are in place;
- access to SECRET STRAP material only;
- police officers and police staff in posts where there is a threat from serious organised crime, provided that Management Vetting (MV) (SOP 4) is applied and ongoing management of the clearance is augmented by an annual security review.

In the above circumstances, an SC clearance should usually be sufficient.

8.3 In the context of this policy, where a DV has been preceded by MV clearance, it also allows regular access to TOP SECRET police assets.

9. Process

9.1 Force Vetting (FV) and National Security Vetting (NSV) are separate processes, designed to counter specific threats to police and government assets respectively. The process for each of HMG's personnel security controls is clearly documented in the Cabinet Office Security Policy Framework (SPF) and this should be referred to for detailed guidance.

9.2 Although the justification for applying FV and NSV is different and must be maintained, there is significant overlap in the sources of information that need to be interrogated in order to grant clearance of either kind. So, where a separate requirement for NSV exists, the interrogation of the common databases which underpin both types of clearance are done only once and checks carried out as part of the FV regime contribute to and are taken into account when considering NSV. The only elements unique to NSV, and therefore those areas which must be applied separately, are the Security Questionnaires, Security Service Check and investigations by trained, specialist Investigating Officers (at DV and, where appropriate, at CTC and SC).

9.3 The order in which FV and NSV are applied is crucial: it is imperative that all the elements of FV are satisfactorily completed before entering into the NSV-related actions. In short, RV is a prerequisite for CTC, MV for SC or DV. This is summarised in the table below:

Force Vetting (underpinned by the Authentication procedure)	**Additional requirements for NSV once FV-related checks have been satisfactorily completed**	**National Security Vetting (underpinned by the BPSS)**
RV	Completion of a Security Questionnaire On-line Security Service Check via Parasol Exceptionally, a subject interview by a trained, specialist Investigating Officer	CTC
MV	Completion of a Security Questionnaire On-line Security Service Check via Parasol Exceptionally, a subject interview by a trained, specialist	SC

	Investigating Officer	
MV	Completion of a Security Questionnaire, DV Financial Questionnaire and DV Supplement Questionnaire Off-line Security Service Check A subject interview by a trained, specialist Investigating Officer and further enquiries	DV

9.4 Individuals requiring a CTC, SC or DV security clearance must complete the appropriate security questionnaire(s) only after the appropriate RV or MV checks have been satisfactorily completed. In this way, individuals are not entering the NSV process until actually required to do so. If this is impracticable and individuals are required to complete the Security Questionnaire(s) at the same time as the FV questionnaire(s), they must be advised that processing of the Security Questionnaire(s) and, therefore, consideration of NSV is conditional on RV or MV being granted.

10. Clearance Decisions

10.1 The criteria for acceptability on national security grounds will be different to FV and it is important to preserve the ability to judge adverse traces based on the appropriate criteria. Risk factors and general considerations, including adjudicative guidelines for NSV clearances are contained in the Cabinet Office Security Policy Framework (SPF). It must also be borne in mind that arrangements for any appeals against refusal or withdrawal of CTC, SC or DV security clearance will require that appropriate criteria have been applied.

10.2 If a decision is taken to refuse RV or MV, the process stops at that point and no action is taken in respect of CTC, SC or DV (i.e. the individual would not be required to complete a Security Questionnaire (or if they have, this information would not go forward) and there would be no check of Security Service records or any other investigations). Any appeal against the refusal or withdrawal of RV or MV would be through FV channels and must in no way impact upon NSV arrangements via the Security Vetting Appeals Panel (SVAP).

10.3 If RV, MV or EMV is granted, and the individual also requires a CTC, SC or DV security clearance, the additional requirements for NSV (summarised in the table above) would then be carried out. Where these checks are satisfactory, CTC, SC or DV would be granted. Where these additional checks lead to a refusal or withdrawal of security clearance, any appeal would be subject to NSV arrangements with an internal appeal and then, if necessary, via the SVAP.

10.4 If CTC, SC or DV clearance is refused or withdrawn an assessment of the individual's suitability to hold RV, MV, EMV or NPPV Level 3 clearance should be conducted, and escalated to the Head of Professional Standards Department if required.

10.5 If an individual is refused security clearance, or has their security clearance withdrawn, the Security Service should be notified immediately by letter which should contain details of the name and date of birth of the individual, and any PARASOL reference number (if known), along with a short summary of reason(s) for the vetting refusal. The letter should be double enveloped with

the outside envelope addressed to: 'The Secretary, PO Box 5656, London EC1A 1AH'. The inner envelope should be marked: 'Attn: C1 Vetting Section'.

10.6 If the Security Service has passed information or an assessment, based on either their own records or material received from a liaison source, they should be notified of the decision to grant or refuse NSV clearance.

10.7 In cases where police officers, members of the special constabulary and police staff are required to resign, resign prior to and in anticipation of misconduct proceedings or are dismissed from the Police Service, their NSV clearance will automatically lapse. In cases involving NSV, the Security Service should be notified immediately and a record created on the force intelligence system so that the matter is flagged on the IMPACT Nominal Index (INI).

11. Appeals

11.1 FV will have its own appeal/review arrangements. For NSV, police forces must have in place an internal appeals process to consider challenges by individuals to adverse security clearance decisions. The process should include an ultimate right of appeal to a nominated senior officer (who is independent of the original decision making process) and provide the individual with the opportunity of a face-to-face interview.

11.2 Where the internal appeals process has been exhausted and the individual remains dissatisfied with the outcome, s/he may seek to appeal to the independent Security Vetting Appeals Panel (SVAP), or may use other legal processes. SVAP is not available to individuals who have been refused NSV clearance as part of a recruitment process (i.e. applicants for appointment where no job offer is made).

12. Ongoing Personnel Security

12.1 The checks and interviews associated with NSV can only provide a snapshot of an individual at a given point in time. It is important that, even for those individuals who are cleared with no adverse information, that vetting information is reviewed and updated on a regular basis.

12.2 Line management has a fundamental role to play in the maintenance of personnel security. Line managers should note any changes or events that might affect the reliability of those who are security cleared and raise any cause for concern with the appropriate senior responsible officer.

12.3 Line managers are supported by two formal processes: annual security review (for all DV and SC posts) and renewals. Both may be used more frequently than mandated below if it is necessary and proportionate to manage a risk or vulnerability presented by an individual.

13. Reviews

13.1 NSV clearances must be subject to periodic reviews:

- in the light of any adverse information received subsequent to the original vetting process;
- to follow up adverse indicators identified in the original vetting process;
- at regular intervals as shown below.

13.2 The following review periods are a minimum standard and NSV clearances may be reviewed more regularly at the discretion of the employer:

- CTC: 10 years (see Aftercare (SOP 10) for guidance relating to non-police personnel);
- SC: 10 years (supported by annual security review);
- SC (Enhanced): 5 years (supported by annual security review);
- DV: initially 5 years and every 7 years thereafter (supported by annual security review) ;

13.3 Where an individual who holds NSV clearance transfers to a post which does not require NSV clearance, the clearance will automatically lapse 12 months after transfer. Should they transfer back to a post requiring NSV clearance within the 12 month period, the force must decide whether to review the clearance or accept it at face value, taking into account overseas residence during the period and the fact that the individual would not have been subject to the usual aftercare arrangements. Should the individual transfer back to a post requiring NSV clearance 12 or more months following the initial transfer, the NSV clearance will have expired and must be renewed.

14. Responsibilities

14.1 This SOP is owned by the ACPO Professional Standards Committee.

14.2 Responsibility for implementing and reviewing the SOP rests with the ACPO National Vetting Working Group.

15. Associated Documents and Policies

- ACPO / ACPOS National Vetting Policy for the Police Community
- Cabinet Office Security Policy Framework (formerly the Manual of Protective Security)
- Authentication SOP 2
- Recruitment Vetting SOP 3
- Management Vetting and Enhanced Management Vetting SOP 4
- Non Police Personnel Vetting SOP 5
- Appeals/Review Procedure SOP 9
- Aftercare SOP 10

ACPO Professional Standards Committee

Standard Operating Procedure Number 7

VETTING INTERVIEWS

Protective Marking	NOT PROTECTIVELY MARKED
Publication Scheme Y/N	Yes
Title	Vetting Interviews
Version	3.0
Summary	This Standard Operating Procedure supports the ACPO / ACPOS National Vetting Policy for the Police Community
Management	ACPO National Vetting Working Group
Author	Carol Benton [Lancashire], Stewart Finlayson [Strathclyde], Jonathan Gupta [Staffordshire], Bob Lane [Warwickshire], Alan McCawley [MPS]
Date created	August 2010
Review date	August 2011

1. Introduction

1.1 This Standard Operating Procedure (SOP) supports the ACPO/ACPOS National Vetting Policy for the Police Community (NVP) and associated documents and policies.

1.2 This is a new SOP.

2. Application

2.1 This SOP comes into force on 1st August 2010.

3. Purpose

3.1 The purpose of conducting vetting interviews with the subject is to obtain a sufficiently clear picture of the subject's past life and current circumstances to satisfy the force of their integrity and that he or she is not, and is unlikely to become, a security risk. Not all applicants will require a vetting interview but they should be conducted where the vetting information collated raises queries or doubts about particular issues. Although vetting interviews may be required in respect of any type of vetting application it is likely that they will be more common in respect of management vetting and enhanced management vetting (SOP 4) and this guidance is written with that in mind. It is based on the Cabinet Office Security Vetting Investigation and Assessment Guide.

3.2 It is advisable that interviews are conducted after departmental, criminal, financial and security record checks have been made to ensure that the interviewer has the fullest possible information prior to the interview. If a vetting interview is conducted before all relevant information is available it may be necessary to conduct a second interview where there remain unresolved doubts.

3.3 Interviews as part of the process to grant National Security DV clearance must only be conducted by suitably trained and accredited personnel.

4. Process

4.1 Thorough preparation is essential and this includes not only assimilating all the relevant documentary information but also establishing an appropriately professional relationship with the subject prior to the interview. The manner in which this is done will set the tone for all subsequent contact.

4.2 The success of the vetting interview, as with other aspects of vetting, depends largely on the honesty of the subject. Lying or concealing the truth or deliberately withholding information when completing application/vetting forms or during a vetting interview is regarded as a very serious matter, whether it comes to light immediately or at some later stage. It is, therefore, a requirement of any vetting interview that, at the beginning, it is made clear to the subject that absolute honesty is required and that deceit at any stage of the process may impact upon their application. It should also be made clear that if subjects' provide information which may give rise to security concerns it does not necessarily mean that their application will be declined – each case is considered on its merits.

4.3 The subject should be taken through the forms they have completed and asked whether there are any inaccuracies which he or she would wish to

correct or whether there have been any changes in circumstances since they were completed. The interviewer should make sure that the subject has understood all the questions asked. Particular attention should be paid to those questions concerning criminal convictions, security information and financial circumstances. The interviewer should be consistent and cover the same relevant areas with all subjects.

4.4 In order to obtain and retain a subject's full co-operation, it is important that interviews do not assume the form of an interrogation but are handled with sensitivity. Those conducting the interview should never make assumptions or display a judgemental stance and, appreciating the sensitivity and importance of the interview, should display unswerving neutrality. It should be remembered that the subject is being asked to discuss matters which they might not discuss even with close family and friends. It is therefore important to establish a rapport with the subject.

4.5 The confidentiality afforded to information generated as a result of a vetting enquiry must be emphasised. The way in which sensitive information is dealt with will dictate the extent to which people are prepared to entrust you with it. The manner of those conducting the interview may be more effective than any verbal assurances about confidentiality.

4.6 The focus of the questions must be on those areas linked to the decision making process – avoid seeking unnecessary detail on non relevant issues.

4.7 Take time to explain to subjects both the principles and process of vetting procedures, and the necessity for enquiries to cover the areas that they do. The reasons for the interview and sensitive nature of some of the questions must be explained to the subject and their consent to proceed sought. If a subject indicates he or she finds it difficult to discuss the matter every effort should be made to discover whether the process might be made easier by a different interviewer (e.g. one of the same sex as the subject) and wherever practicable such requests should be accommodated and documented.

4.8 The rationale for discussing sensitive matters at a vetting interview, for example, disability, faith and race issues, would need to be explained to satisfy the subject that these issues in themselves would not preclude a successful vetting process. To some, even discussing these issues raises fears of discrimination.

4.9 Any issues revealed which relate to the subject's health should be referred to Occupational Health for a recommendation.

4.10 If a subject absolutely refuses to discuss a relevant matter it will be necessary to point out that the force will have no alternative but to take this into account in reaching a decision and that this might, ultimately, lead to the refusal of clearance.

4.11 Whilst being organised and having planned adequately those conducting interviews should also be prepared to be flexible to meet unexpected demands. Whilst there will be a basic interview structure in mind, allowing the subject free rein to express his or her views can be a useful source of information.

4.12 Always conclude the interview by seeking to establish that the subject is content with the manner in which it has been conducted. This provides an opportunity to clear up any misunderstanding, provides feedback about the

performance of the interviewer and reduces the likelihood of a subsequent complaint.

4.13 Subsequent reports or interview notes should be framed in a way which is clearly free from any subjective value-judgements. They should include the rationale/evidence for making/reaching a particular decision/conclusion.

4.14 The areas to be explored will vary between subjects but may include one or more of the following areas:

- Career to date including satisfaction/dissatisfaction with the employer;
- Relationships (e.g. marriage/co-habitation, family, friends and associates);
- Personal circumstances (e.g. domestic arrangements);
- Lifestyle (e.g. foreign travel and contacts, drug and alcohol use, hobbies, sports, study);
- Criminal activity;
- Personal beliefs (e.g. political extremism);
- Actual or potential conflicts of interest;
- Financial circumstances.

4.15 Care should be taken to ensure that legislative constraints, such as the Data Protection Act, are not breached as part of the interview process.

5. Responsibilities

5.1 This SOP is owned by the ACPO Professional Standards Committee.

5.2 Responsibility for implementing and reviewing the Standard Operating Procedure rests with the ACPO National Vetting Working Group.

6. Associated Documents and Policies

- ACPO / ACPOS National Vetting Policy for the Police Community
- Security Policy Framework (SPF)
- Cabinet Office Security Vetting Investigation and Assessment Guide
- Management Vetting and Enhanced Management Vetting SOP 4

ACPO Professional Standards Committee

Standard Operating Procedure Number 8

CONVICTIONS and CAUTIONS CRITERIA

Protective Marking	NOT PROTECTIVELY MARKED
Publication Scheme Y/N	Yes
Title	Convictions and Cautions Criteria
Version	3.0
Summary	This Standard Operating Procedure supports the ACPO / ACPOS National Vetting Policy for the Police Community
Management	ACPO National Vetting Working Group
Author	Carol Benton [Lancashire], Stewart Finlayson [Strathclyde], Jonathan Gupta [Staffordshire], Bob Lane [Warwickshire], Alan McCawley [MPS]
Date created	August 2010
Review date	August 2011

1. Introduction

1.1 This Standard Operating Procedure (SOP) supports the ACPO / ACPOS National Vetting Policy (NVP) for the Police Community (NVP) and associated documents and policies.

1.2 This is a new Standard Operating Procedure.

2. Application

2.1 This SOP comes into Force on 1st August 2010.

2.2 This SOP applies to all levels of Force Vetting.

3. Purpose

3.1 This SOP is based on the following principles:

- The public is entitled to expect that police forces will recruit people who demonstrate the highest standards of professional conduct, honesty and integrity;
- Those who work for, and with, police forces can be vulnerable to pressure from criminals and others to disclose information;
- Convictions, cautions and other material information which reflects on personal integrity must be revealed by police officers and others in the evidential chain, in accordance with the Crown Prosecution Service (CPS) Prosecution Team Disclosure Manual, to the CPS on every occasion that they submit a statement of evidence in a criminal case. This information will be used by the CPS to assess the strength of the individual's evidence and, if the case proceeds, it is likely then to be disclosed to the defence and may be used in open court to attack the credibility of the officer. Such an occurrence could undermine the integrity of the evidence, the witness and the force;
- Police forces should not recruit people with convictions, cautions and judicial or other formal disposals, which may call in to question the integrity of the applicant or the service;
- Each case must be dealt with on its individual merits.

3.2 In this guidance the term 'caution' includes reprimands, formal warnings and final warnings which must be declared regardless of the date of the 'caution'. Other forms of restorative justice are also included. The term 'convictions' includes 'spent' convictions. The Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975 provides that the Act shall not apply to the police service. Police forces are therefore entitled to ask all prospective applicants for appointment to or direct employment by a police force, or third parties employed for the purposes of, or to assist, a Constable of a police force to reveal spent convictions during the recruitment or vetting process. This does not apply to the spent convictions of applicants' families or associates.

3.3 Cases of criminal/anti-social behaviour where the case disposal has been by way of fixed penalty notice(s) should also be taken into consideration. For vetting purposes, fixed penalty notices are to be treated as a caution.

4. Process

Recruitment Vetting

4.1 Before recruiting anyone to work in a police force thorough checks must be undertaken to ascertain whether anything is known to the detriment of the applicant, his/her spouse or partner, close relatives, in-laws, or those residing or associating with the applicant and any self declared or discovered criminal associations, which could heighten vulnerability, bring discredit upon, or otherwise cause embarrassment to the police service.

4.2 Checks on the PNC/CHS/CIS, force crime information system, local intelligence, counter terrorism databases, and other relevant non-conviction database systems will be appropriate for the applicant and their spouse or partner, close relatives, in-laws, or those residing or associating with the applicant and any self declared or discovered criminal associations.

4.3 Other force intelligence checks should be conducted on the applicant and others. The IMPACT Nominal Index (INI) should be used to achieve this purpose, as per the provisions of SOP 13.

4.4 Such checks should be conducted promptly to avoid delays in processing the applications and forces have agreed to a reciprocal turn round of such requests within 14 calendar days.

4.5 Where appropriate, searches should also be made against Military and Police Professional Standards databases.

5. Criminal Convictions/Cautions Criteria

5.1 The Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975 provides that the Act shall not apply to the police service. Police forces are therefore entitled to ask all prospective applicants for appointment to or direct employment by a police force, or third parties employed for the purposes of, or to assist, a Constable of a police force to reveal spent convictions during the recruitment or vetting process. This does not apply to the spent convictions of applicants' families or associates.

5.2 The convictions criteria to be applied to recruitment vetting can be found at Appendix A.

5.3 In view of the wide range of duties now carried out by police staff the vetting criteria identified at Appendix A, must be applied equally to the recruitment of police officers, police staff and members of the special constabulary.

5.4 The criminal convictions and cautions criteria defined by this SOP must be used to assess each application on an individual basis. Eligibility will depend on the nature and circumstances of the offence. It is not possible to set out a full list of convictions that will preclude a person from joining the police service. Each case will be considered on its merits, and if the offence is deemed sufficiently serious a person will be rejected irrespective of age at the time of offending. Force Vetting Units (FVU) should base their decision on the available information. There is no obligation upon the FVU to reinvestigate the allegation.

5.5 There may be circumstances where an individual does not fall within the criteria, but whose suspected involvement in crime, or criminal associations, make an offer of appointment inappropriate.

5.6 The requirements Chapter 18 of the Crown Prosecution Service Prosecution Team Disclosure Manual must be considered when making decisions on suitability.

5.7 All decisions must be clearly documented and must include the rationale behind the decision.

6. Application

6.1 Applicants must declare if they have ever been investigated, arrested, summonsed, charged, cautioned or convicted for any offence by any UK or non-UK Police Force, Law Enforcement Agency or any other statutory prosecuting authority or agency – this includes, but is not limited to:-

- Traffic offences (including fixed penalty notices excluding parking);
- Receipt of an absolute/conditional discharge or bindover;
- Receipt of a reprimand, warning, final warning or caution or other form of restorative justice as an adult or juvenile;
- Being the subject of an Anti-Social Behaviour Order, Football Spectator Banning Order, Risk of Sexual Harm Order, Harassment Order;
- Being issued with a Penalty Notice for Disorder or other Fixed Penalty Notice (other than for parking).

In addition, the following must also be declared;

- Any involvement with the military authorities on disciplinary matters (whether involving court martial or not);
- Involvement in a criminal investigation as a suspect (whether or not this has led to a prosecution);
- Association with criminals;
- Being subject of Service Confidence Procedure;
- Any other matters which might be relevant.

6.2 Applicants must be advised to carefully read the appropriate notes for guidance when completing application forms.

6.3 Applicants should not be informed that they have been 'successful pending the satisfactory completion of security checks'. They should be informed that any offer of appointment is made on the satisfactory completion of all medical, reference and vetting procedures.

Undisclosed Convictions

6.4 Where an applicant has failed to disclose a conviction, caution or other relevant information as outlined above, his or her application should be rejected at this stage on the grounds of honesty and integrity.

Outstanding Charges and Summonses

6.5 Where an individual discloses any outstanding investigation the decision should be deferred until the outcome is known, at which point it will be considered in accordance with this guidance.

HM Forces

6.6 Serving members of the armed forces who are convicted of any criminal offence by a military tribunal will normally have any such offence recorded on the Police National Computer (PNC). This will include any aspect of a conditional discharge. In certain circumstances, the PNC is not updated. Therefore, it is essential that a military check is undertaken on all applicants who have previously served in the armed forces.

Relatives and Associates with Criminal Convictions or Cautions

6.7 Where relatives or the associates of an applicant are found to have unspent convictions or cautions for recordable offences, or there is intelligence suggesting involvement in criminal activity, the following should be considered:

- The likelihood that the applicant's performance and discharge of duty will be adversely affected e.g. through adverse pressure or a conflict of interests;
- The nature, number and seriousness of the offences or involvement in criminal activity and the time over which these took place;
- Whether the circumstances are likely to bring discredit to or embarrass the police service or police force.

6.8 A decision that an applicant is 'unsuitable' on the basis of relatives' convictions, intelligence material or his/her criminal associations should be taken by the FVO. The results of checks on relatives and associates must not be disclosed to an applicant. (See SOP 16).

Non-Police Personnel

6.9 There are different levels of non-police personnel vetting and the convictions and cautions criteria to be applied will vary according to the level of access to police assets and/or information. The criteria identified at Appendix A should be applied to NPPV Levels 2 and 3, whilst the criteria identified at Appendix B should be applied to NPPV Level 1.

6.10 All decisions must be clearly documented and any deviations from the guidance in this SOP should be carefully considered and authorised at the appropriate level.

7. Responsibilities

7.1 This SOP is owned by the ACPO Professional Standards Committee.

7.2 Responsibility for implementing and reviewing the SOP rests with the ACPO National Vetting Working Group.

8. Associated Documents and Policies

- ACPO / ACPOS National Vetting Policy for the Police Community
- Security Policy Framework (SPF)
- National Police Improvement Agency (NPIA) Circular 01/2010
- CPS Prosecution Team Disclosure Manual
- The Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975
- Recruitment Vetting SOP 3
- Non-Police Personnel Vetting SOP 5
- Risk Assessments SOP 16
- Adverse Information and Judicial Findings SOP 17

ACPO Professional Standards Committee

Standard Operating Procedure Number 9

APPEALS and REVIEW PROCEDURE

Protective Marking	NOT PROTECTIVELY MARKED
Publication Scheme Y/N	Yes
Title	Appeals and Review Procedure
Version	3.0
Summary	This Standard Operating Procedure supports the ACPO / ACPOS National Vetting Policy for the Police Community
Management	ACPO National Vetting Working Group
Author	Carol Benton [Lancashire], Stewart Finlayson [Strathclyde], Jonathan Gupta [Staffordshire], Bob Lane [Warwickshire], Alan McCawley [MPS]
Date created	August 2010
Review date	August 2011

1. Introduction

1.1 This Standard Operating Procedure (SOP) supports the ACPO/ACPOS National Vetting Policy for the Police Community (NVP) and associated documents and policies.

1.2 This is a new SOP.

2. Application

2.1 This SOP comes into force on 1st August 2010.

3. Purpose

3.1 The purpose of this SOP is to confirm the appeals/review processes in respect of adverse vetting decisions.

4. Process

Scope of the Appeal and Review Processes

4.1 Where applicants are notified of an adverse vetting decision, they should be informed of the existence of the appeal / review procedures.

4.2 The following processes are to be used for appeals against, or reviews of, adverse vetting decisions; that is the refusal, withdrawal or suspension of clearance, and applies to the following forms of vetting:

- Recruitment Vetting (RV)
- Management Vetting (MV)
- Enhanced Management Vetting (EMV)
- Non Police Personnel Vetting (review only)
- National Security Vetting (NSV) at all levels
- Transferees and Rejoiners (review only)

4.3 Requests for an appeal or a review must be made in writing and must be from the applicant themselves, or endorsed by the applicant.

4.4 When a written request for an appeal or review has been received, where possible, individuals will be provided with the reason for their refusal in writing, unless doing so would be likely to:

- Damage national security;
- Result in the force breaking any law;
- Frustrate the prevention or detection of crime;
- Impede the apprehension or prosecution of offenders;
- Result in the disclosure of sensitive information;
- Breach the confidentiality of any information provided in confidence.

4.5 It should be noted that the Chief Officer reserves the right to refuse appointment without giving reason under Section 6 Police Act 1996 and the Police (Scotland) Act 1967.

5. Procedure

Appeals

Recruitment Vetting (RV), Management Vetting (MV) and Enhanced Management Vetting (EMV)

5.1 If an internal applicant disputes the decision to refuse, withdraw or suspend RV, MV or EMV clearance, a letter of appeal must be forwarded via the Force Vetting Officer (FVO) to an officer of ACPO/ACPOS rank, or other nominated individual who has not been involved in the original decision, within 14 days of receipt of a written notification of the decision. The officer of ACPO/ACPOS rank will consider the case within 28 days of receipt of the letter of appeal. The individual will be given the opportunity to make personal representation and may be accompanied by a friend or staff association or Trade Union representative. The officer conducting the appeal will inform the applicant in writing of the result of the appeal as soon as practicable after the decision has been made. Any decision reached will be final.

5.2 Appeals by members of Police Staff should be considered by a panel comprising an ACPO(S) member and a member of the relevant Police Authority, reflecting that the Police Authority is the employer for Police Staff.

5.3 External applicants for RV, MV and EMV posts have no right of appeal against a decision not to grant them vetting clearance. It is suggested that they should, however, be given the opportunity to have the decision reviewed (see below).

National Security Vetting

5.4 A decision not to grant any level of NSV clearance can only be challenged where the decision will have a prejudicial effect on the individual's current employment. Where clearance is refused as part of a recruitment process, it cannot be challenged.

5.5 For individuals who are already appointed or employed, forces should have in place an internal appeals process to consider challenges by individuals to adverse security clearance decisions. Police staff appeals must have the involvement of a member of the Police Authority.

5.6 Where internal appeals procedures have been exhausted, but the individual remains dissatisfied with the outcome, they may seek to appeal to the independent Security Vetting Appeals Panel (SVAP), or may use other legal processes. SVAP is not available to individuals who have been refused NSV clearance as part of a recruitment process.

Counter Terrorist Check (CTC)

5.7 Individuals who have already been appointed who are refused CTC clearance have the right to appeal within force to a nominated officer of ACPO rank and finally to the independent SVAP. For cases involving members of Police Staff, the appeal in force should be heard by a panel consisting of a nominated officer of ACPO rank and member of the Police Authority.

Security Check (SC)

5.8 Individuals who have already been appointed who pass the MV procedure, but are subsequently refused SC clearance, can appeal within force in the first instance, to a nominated officer of ACPO Rank (the Scottish Government Appeals Panel in Scotland), and finally to the independent SVAP. For cases involving members of Police Staff, the appeal in force should be heard by a panel consisting of a nominated officer of ACPO rank and member of the Police Authority.

5.9 External applicants for SC designated posts have no right of appeal either within the force, or to the independent SVAP.

Developed Vetting (DV)

5.10 Appeals by serving individuals against a decision by the nominated ACPO Officer, or the Departmental Security Officer (DSO), not to grant DV clearance, are heard initially by the Chief Officer and finally by the independent SVAP. In cases where the applicant is the Chief Officer, direction should be sought from the Home Office Departmental Security Officer (DSO) or Scottish Government.

Reviews

5.11 There is no right to a review for any applicant. However, it is suggested as best practice, that a review procedure is made open to the following;

- RV (external applicants);
- MV (external applicants)
- EMV (external applicants)
- NPPV
- Transferees and rejoiners;

Recruitment Vetting

5.12 External applicants for recruitment to the police community have no right of appeal against a decision not to offer them appointment. However, it is suggested as best practice that a review procedure is made available. There is no right to a personal hearing.

5.13 Requests for review should be made in writing within 28 days of receiving notification of the decision not to grant clearance. The review should be conducted by a nominated individual not previously involved in the case, who has a working knowledge of vetting policies. The reviewer will view the case file together with any additional information provided by the applicant within 28 days of receipt of the letter, and will communicate the review decision in writing, as soon as practicable following the decision. Any decision made will be final.

5.14 All reviews must be made in line with the guidance contained within this policy. A documented rationale of the review decision must be maintained with the vetting file for audit trail purposes.

MV and EMV (External Applicants)

5.15 External applicants for recruitment to the police community have no right of appeal against a decision not to offer them employment or appointment.

However, it is suggested as best practice that a review procedure is made available. There is no right to a personal hearing.

5.16 A letter requesting a review should be forwarded to the nominated officer within 14 days of receipt of written notification of the decision. The review will be conducted by a nominated individual who has not been involved in the original decision, who will review the original decision within 28 days of receipt of the letter of review and will provide the applicant with a written statement outlining the result of the review. The decision reached will be final. There is no right to personal representation at a review.

5.17 All reviews must be made in line with the guidance contained within this policy. A documented rationale of the review decision must be maintained with the vetting file for audit trail purposes.

NPPV

5.18 Applicants for NPPV have no right of appeal against a decision not to grant the relevant level of clearance. However, it is suggested as best practice that a review procedure is made available. There is no right to a personal hearing.

5.19 Requests for review should be made in writing within 28 days of receiving notification of the decision not to grant clearance. The review should be conducted by an individual not previously involved in the case, who has a working knowledge of vetting policies. The reviewer will view the case file together with any additional information provided by the applicant within 28 days of receipt of the letter, and will communicate the review decision in writing, as soon as practicable following the decision. Any decision made will be final.

5.20 All reviews must be made in line with the guidance contained within this policy. A documented rationale of the review decision must be maintained with the vetting file for audit trail purposes.

Transferees & Re-joiners

5.21 Transferees and rejoiners have no right of appeal against the vetting decision. However, it is suggested as best practice that a review procedure is made available.

5.22 Requests for review should be made in writing within 28 days of receiving notification of the decision not to grant clearance. The review should be conducted by an individual not previously involved in the case, who has a working knowledge of vetting policies. There is no right to a personal hearing. The reviewer will view the case file together with any additional information provided by the applicant within 28 days of receipt of the letter, and will communicate the review decision in writing, as soon as practicable following the decision. Any decision made will be final.

5.23 All reviews must be made in line with the guidance contained within this policy. A documented rationale of the review decision must be maintained with the vetting file for audit trail purposes.

6. Responsibilities

6.1 This SOP is owned by the ACPO Professional Standards Committee.

6.2 Responsibility for implementing and reviewing this SOP rests with the ACPO National Vetting Working Group.

7. Associated Documents and Policies

- ACPO / ACPOS National Vetting Policy for the Police Community
- Security Policy Framework (SPF)
- Police Act 1996
- Police (Scotland) Act 1967

ACPO Professional Standards Committee

Standard Operating Procedure Number 10

AFTERCARE and RENEWAL OF CLEARANCE

Protective Marking	NOT PROTECTIVELY MARKED
Publication Scheme Y/N	Yes
Title	Aftercare and Renewal of Clearance
Version	3.0
Summary	This Standard Operating Procedure supports the ACPO / ACPOS National Vetting Policy for the Police Community
Management	ACPO National Vetting Working Group
Author	Carol Benton [Lancashire], Stewart Finlayson [Strathclyde], Jonathan Gupta [Staffordshire], Bob Lane [Warwickshire], Alan McCawley [MPS]
Date created	August 2010
Review date	August 2011

1. Introduction

1.1 This Standard Operating Procedure (SOP) supports the ACPO/ACPOS National Vetting Policy for the Police Community (NVP) and associated documents and policies.

1.2 This is a new SOP.

2. Application

2.1 This SOP comes into force on 1st August 2010.

2.2 Whilst all levels of vetting clearance should be subject to an aftercare process, only specified levels are time limited and require renewal.

3. Purpose

3.1 Aftercare is arguably the most important part of any enhanced vetting process. Vetting is based on a 'snapshot in time'. The subject's personal circumstances can, and often will, be subject to a *significant change* over time and this may affect their suitability to maintain their clearance. It is therefore vital that the individual's suitability is assessed over time through a comprehensive aftercare regime. Specified levels of clearance are time limited and require renewal after that time period has passed.

3.2 It is the responsibility of the Force Vetting Officer (FVO) to ensure that aftercare / renewals of clearances are completed.

4. Process

Aftercare

4.1 All individuals who are subject to the vetting process must report any changes in their personal circumstances which may be of relevance to their clearance. Such changes may include, but are not limited to:

- change of home address;
- change in partner;
- co-habitant details;
- involvement in a criminal investigation as a suspect;
- arrest for criminal offence;
- conviction for a criminal offence;
- receipt of fixed penalty notice;
- bankruptcy;
- adverse County/Sheriff Court Judgement;
- entry into an Individual Voluntary Arrangement (IVA);
- known / suspected criminal association;
- relevant changes in medical condition – to be notified and acted upon by Occupational Health.

4.2 Due to the sensitive nature of information which may be disclosed as part of the aftercare process, it is important that those subject to vetting have sufficient trust in the confidentiality of the procedures to enable full and frank disclosure.

4.3 Whilst individuals should be able, and encouraged, to make such disclosures at any time following vetting clearance, those holding Management Vetting (MV), Enhanced Management Vetting (EMV), Security Check (SC) and Developed Vetting (DV) clearance should also be subject to an Annual Security Review. The standard questionnaires for these are attached as Appendix 1.

4.4 The FVO will reserve the right to conduct personal interviews with those holding designated posts as part of the aftercare process.

Renewals

4.5 Certain levels of vetting clearance are subject to renewal. The table below shows which levels require renewal and the timescales attached:

Clearance Level	Renewal Period
RV	10 years
CTC	10 years 5 years for Non-Police Personnel
MV	5 years
EMV	5 years
SC	10 years
SC Enhanced	5 years
DV	Initially 5 years following initial clearance and then must be renewed every 7 years thereafter.
NPPV 1	12 months
NPPV 2	3 years
NPPV 3	5 years

4.6 Where an individual who holds National Security Vetting (NSV) clearance transfers to a post which does not require NSV clearance, the clearance will lapse 12 months after transfer. Should they transfer back to a post requiring NSV clearance 12 or more months following the initial transfer, the NSV clearance will have expired and must be renewed.

Adverse Information

4.7 Where the aftercare process reveals a change in circumstances which may have a prejudicial effect on the individual's suitability to maintain the relevant level of clearance, consideration should be given to withdrawal of that clearance. Only in the most serious of cases should clearance be withdrawn.

4.8 Decisions relating to the withdrawal/maintenance of vetting clearance following the discovery of adverse information must be clearly documented and kept on the subject's vetting file.

4.9 Where the Line Manager's assessment contains negative responses, these should be fully investigated and verified before being relied upon to support any action in relation to vetting clearance.

4.10 The aftercare process may also reveal information which relates to a breach of Police (Conduct) Regulations/Standard of Professional Behaviour, about which the force was previously unaware. In such circumstances, the matter must be immediately referred to the Head of Professional Standards for appropriate action. In addition, any consideration in relation to the withdrawal of clearance in such circumstances should be made in consultation with the Head of Professional Standards as doing so may prejudice an investigation.

4.11 Forces should have in place documented appeals procedures for cases where clearance is withdrawn.

4.12 Where NSV clearance is withdrawn the Security Services must be informed (see SOP 6).

5. Responsibilities

5.1 This SOP is owned by the ACPO Professional Standards Committee.

5.2 Responsibility for implementing and reviewing the SOP rests with the ACPO National Vetting Working Group.

6. Associated Documents and Policies

- ACPO / ACPOS National Vetting Policy for the Police Community
- Security Policy Framework (SPF)
- Recruitment Vetting SOP 3
- Management Vetting and Enhanced Management Vetting SOP 4
- Non-Police Personnel Vetting SOP 5
- National Security Vetting SOP 6
- Appeals/Review Procedure SOP 9

ACPO Professional Standards Committee

Standard Operating Procedure Number 11

TRANSFEREES AND RE-JOINERS

Protective Marking	NOT PROTECTIVELY MARKED
Publication Scheme Y/N	Yes
Title	Transferees and Re-joiners
Version	3.0
Summary	This Standard Operating Procedure supports the ACPO / ACPOS National Vetting Policy for the Police Community
Management	ACPO National Vetting Working Group
Author	Carol Benton [Lancashire], Stewart Finlayson [Strathclyde], Jonathan Gupta [Staffordshire], Bob Lane [Warwickshire], Alan McCawley [MPS]
Date created	August 2010
Review date	August 2011

1. Introduction

1.1 This Standard Operating Procedure (SOP) supports the ACPO/ACPOS National Vetting Policy for the Police Community (NVP) and associated documents and policies.

1.2 This is a new SOP.

2. Application

2.1 This SOP comes into force on 1st August 2010.

2.2 This SOP applies to:

- individuals who wish to transfer from one Police Force to another;
- those who have resigned from the Police Service and wish to rejoin at a later date;
- those rejoining under the 30+ scheme ;
- those returning from secondment;

Additionally, it also applies to:

- Police Staff who have been dismissed;
- Police Officers who have been dismissed;
- Police Officers who were required to resign;

and who have successfully appealed against the original sanction and have been re-instated.

2.3 It also includes any other extended period of absence.

2.4 It does not apply to those who have been absent from force for a significant period of time on medical grounds.

3. Purpose

3.1 The purpose of this SOP is to ensure Police Officers, members of the Special Constabulary or Police Staff who are rejoining their previous force, joining another after a break in service, or are transferring to another force have been Force Vetted and National Security Vetted (NSV) to the appropriate levels, as set within the NVP, and that the vetting is current and not historical.

3.2 It is a requirement to ensure that the integrity of the individual is beyond question and that there are no outstanding complaints or matters currently under investigation.

3.3 Occasions have arisen where Service Confidence or similar procedures have been instigated for transferees who had commenced duty in the 'receiving force' where concerns have been raised as to their honesty and integrity whilst serving with the 'parent force'. In some cases, the motivation for the transfer has been the avoidance of detection within the 'parent force', with some transferees subject to active Professional Standards investigations. A number of transferees have had to return to their 'parent force' to attend hearings in respect of serious disciplinary offences.

3.4 There have also been occasions when officers have transferred from one force to another and failed to declare a criminal matter which their parent force was unaware of and which would be a clear reason for failing their

application, in addition to leading to a discipline board and possible dismissal within their current force.

3.5 Where officers transfer between forces their previous vetting file(s) should transfer with them.

3.6 **It should be noted that, where Police Officers, members of the Special Constabulary or Police Staff have been dismissed/required to resign and subsequently return to work, the commencement of appointment cannot be delayed in the absence of security vetting**. Where such Police Officers, members of the Special Constabulary or Police Staff subsequently return to work and vetting checks reveal adverse information covering the dismissal period the Professional Standards Department will be notified. They will consider if the Police Officer, member of the Special Constabulary or Police Staff has breached regulations or their conditions of service and take action accordingly. If the adverse information relates to National Security Vetting the appropriate measures should be taken immediately.

4. Process

4.1 Under Home Office procedures, transferee application forms for police officers up to the rank of Superintendent[1], are sent directly by applicants to the 'receiving force' without notification to the 'parent force'. The only contact applicants have with their 'parent force' is to obtain copies of their last two personal appraisal/development records, sickness record for the previous three years, print-outs of complaints and misconduct records, and awards and commendations. Applicants are required to collate this information and send it directly to the 'receiving force' recruitment unit.

4.2 A procedure has been devised to synchronise with guidance issued by the Home Office and the possible introduction of a new Home Office Transferee Application Form to be adopted by forces for transfers up to the rank of Superintendent.

4.3 Transfers between forces are voluntary arrangements with no right of appeal. However, there can be a request for a review of the procedure and decision. This must be made in writing to an officer of ACPO/ACPOS rank, or other nominated individual who has not been involved in the original decision. All decisions made will be final.

4.4 On occasions, applicants may have previously applied to join the receiving force, either on initial recruitment or as a transferee, and had their application rejected. In these circumstances forces should review whether the original grounds for rejection remain valid.

4.5 For Police Officer re-joiners, Police Staff and members of the Special Constabulary, applications will be routed through the 'parent force' Personnel/HR Departments or in line with existing local force arrangements. Forces should put in place a process for clearly identifying previous police service, which will initiate the checks as detailed below. In addition, such individuals should be specifically asked about previous police service, and careful consideration given to the reasons provided for leaving and applying to rejoin.

[1] Includes police forces in England, Scotland, Wales, PSNI and BTP.

5. Checks

5.1 All checks as detailed in the Recruitment Vetting SOP (SOP 3) should be carried out as a minimum.

5.2 Individuals should not be permitted to transfer or rejoin without consultation with both the parent and receiving force Professional Standards Department, and with the Force Vetting Officer/Unit, irrespective of the length of time absent from the force.

5.3 Where the transferee holds National Security Vetting (NSV) clearance then the clearance level should be transferred provided there has been no break in service and it can be demonstrated that the aftercare requirements have been satisfied. A copy of the vetting file should transfer with the officer.

5.4 It is important that the full Professional Standards record of the individual is disclosed as well as any concerns over integrity through the Health Check. It is accepted that any concerns over integrity may not be disclosed between Force Vetting Units and that disclosure may be confined between the two respective Professional Standards Departments. The process as highlighted within Appendix A should be adopted.

6. Refusal

6.1 Chief Officers retain the right to reject any application without stating a reason under Section 6 of the Police Act 1996 and the Police (Scotland) Act 1967.

6.2 Where Police Officers or Police Staff return to work from secondment and vetting checks reveal adverse information covering the secondment period the Professional Standards Department will be notified. They will consider if the Police Officer or member of Police Staff has breached regulations or their conditions of service and take action accordingly.

7. Appeals

7.1 Transferees and re-joiners have no right of appeal against the vetting decision. However, it is suggested as best practice that a review procedure is made available.

8. Reviews

8.1 Requests for a review should be made in writing within 28 days of receiving notification of the decision not to grant clearance. The review should be conducted by an individual not previously involved in the case, who has a working knowledge of vetting policies. There is no right to a personal hearing. The reviewer will view the case file together with any additional information provided by the applicant within 28 days of receipt of the letter, and will communicate the review decision in writing, as soon as practicable following the decision. Any decision made will be final.

8.2 All reviews must be made in line with the guidance contained within this policy. A documented rationale of the review decision must be maintained with the vetting file for audit trail purposes.

9. Responsibilities

9.1 This SOP is owned by the ACPO Professional Standards Committee.

9.2 Responsibility for implementing and reviewing the SOP rests with the ACPO National Vetting Working Group.

10. Associated Documents and Policies

- ACPO / ACPOS National Vetting Policy for the Police Community
- Security Policy Framework (SPF)
- Recruitment Vetting SOP 3
- National Security Vetting SOP 6
- Aftercare/Renewal of Clearance SOP 10
- Police Act 1996
- Police (Scotland) Act 1967

ACPO Professional Standards Committee

Standard Operating Procedure Number 12

CAREER BREAKS

Protective Marking	NOT PROTECTIVELY MARKED
Publication Scheme Y/N	Yes
Title	Career Breaks
Version	3.0
Summary	This Standard Operating Procedure supports the ACPO / ACPOS National Vetting Policy for the Police Community
Management	ACPO National Vetting Working Group
Author	Carol Benton [Lancs], Stewart Finlayson [S'clyde], Jonathan Gupta [Staffs], Bob Lane [Warwicks], Alan McCawley [MPS]
Date created	August 2010
Review date	August 2011

1. Introduction

1.1 This Standard Operating Procedure (SOP) supports the ACPO/ACPOS National Vetting Policy for the Police Community (NVP) and associated documents and policies.

1.2 This is a new SOP.

2. Application

2.1 This SOP comes into force on 1st August 2010.

2.2 This SOP relates to the vetting of individuals specifically returning from a career break.

2.3 Career break and extended periods of absence policies and procedures are owned and administered by force HR departments

2.4 A career break is an extended period of leave from work that begins with an intention to resume working at an agreed date in the future and is open to both Police Officers and Police Staff.

2.5 The reasons for requesting a career break will generally fall within one of the following categories:

- Personal Development – e.g. extended periods of travel or voluntary service overseas;
- Education – e.g. to pursue full time education; and
- Family care/carer responsibilities - e.g. to care for children or dependants.

2.6 Individuals on career break will continue to be regarded as serving police officers/employees of the force, and remain subject to Police Regulations and force Conditions of Service.

2.7 Acts of misconduct committed whilst on a career break will be dealt with in accordance with Police Regulations and force Conditions of Service. The individual, regardless of location, must report any changes in personal circumstances, involvement in legal proceedings or criminal investigations, allegations or convictions.

3. Purpose

3.1 The purpose of this SOP is to ensure all Police Officers and Police Staff who return to the service following a career break are security cleared to the required levels as designated by the NVP.

4. Process

4.1 Individuals who have been on a career break will submit a full vetting application, including a declaration indicating whether or not they have come to the attention of the police or relevant Law Enforcement Agencies, through their HR Manager prior to their return. The application will be clearly marked indicating the length of time the Police Officer or member of Police Staff has been on a career break together with the details of any time spent out of the country.

4.2 If any adverse information likely to give rise to disciplinary action or misconduct proceedings is found or declared during the vetting process the Force Vetting Officer (FVO) should immediately notify the Professional Standards Department. Consideration should then be made as to whether appropriate action against the Police Officer or member of Police Staff is to be taken.

4.3 If the adverse information relates to National Security Vetting (NSV) the appropriate measures should be taken immediately (see SOP 6).

5. Responsibilities

5.1 This SOP is owned by the ACPO Professional Standards Committee.

5.2 Responsibility for implementing and reviewing the SOP rests with the ACPO National Vetting Working Group.

Associated Documents and Policies

- ACPO / ACPOS National Vetting Policy for the Police Community
- Security Policy Framework (SPF)
- Recruitment Vetting SOP 3
- National Security Vetting SOP 6
- Other Force Vetting Checks SOP 13

ACPO Professional Standards Committee

Standard Operating Procedure number 13

OTHER FORCE VETTING CHECKS (IMPACT Nominal Index and PND)

Protective Marking	NOT PROTECTIVELY MARKED
Publication Scheme Y/N	Yes
Title	Other Force Vetting Checks (INI and PND)
Version	3.0
Summary	This Standard Operating Procedure supports the ACPO / ACPOS National Vetting Policy for the Police Community
Management	ACPO National Vetting Working Group
Author	Carol Benton [Lancashire], Stewart Finlayson [Strathclyde], Jonathan Gupta [Staffordshire], Bob Lane [Warwickshire], Alan McCawley [MPS]
Date created	August 2010
Review date	August 2011

1. Introduction

1.1 This Standard Operating Procedure (SOP) supports the ACPO/ACPOS National Vetting Policy for the Police Community (NVP) and associated documents and policies.

1.2 This is a new SOP.

2. Application

2.1 This SOP comes into force on 1st August 2010.

3. Purpose

3.1 The purpose of the Other Force Vetting Checks (IMPACT Nominal Index) SOP is to ensure that, for all levels of vetting, enquiries are made against relevant intelligence and information databases.

3.2 The requirements for Police Officer Recruitment Vetting are outlined in National Police Improvement Agency (NPIA) 01/2010, entitled, 'Police Officer Recruitment: Eligibility Criteria for the Role of Police Constable'. The Circular includes guidance on the checks to be undertaken prior to the acceptance of applicants. These include qualifications, nationality, finances, criminal convictions, armed services checks and references.

3.3 Forces should ensure that vetting enquiries are made across all Force areas, by utilising the IMPACT Nominal Index (INI). Forces should support each other in ensuring the integrity of all vetting processes by responding promptly to such requests following a positive trace on the INI, or as a result of an LIO check in forces which do not fully upload to INI.

4. Process

4.1 Prior to any request for information being sent to another force, it is imperative that a PNC check be carried out on the individual(s) to be checked. This will prevent unnecessary checks being carried out where an individual would ordinarily fail vetting.

4.2 All forces have been provided with Impact Nominal Index (INI) licenses specifically for vetting. The INI should be used to make enquiries in other force areas. Certain forces do not upload all relevant data onto INI, where an individual has resided in such a force area local intelligence enquiries should be undertaken. This practice should continue until all forces upload all data to INI.

4.3 INI checks should be conducted on the applicant and others named on the application form, regardless of where they have resided.

4.4 Where access to INI has been granted searches using INI should be the means of checking if anything is known about an individual. The check should be conducted on the applicant and any other individual named on the vetting documentation or, where information has given rise to the need to expand the search, any other individual discovered during vetting enquiries. The search should be undertaken using the 'find nominal' field.

4.5 Again, in the absence of INI, where the application has disclosed previous armed services employment, or such employment has been discovered, a check must be carried out with the relevant service.

4.6 Upon discovery that there is information held elsewhere within the UK not provided for within INI or where access to INI has not been granted then the request for information should be extended to include that force area where the information is held.

4.7 Any positive 'traces' on INI must be followed up with a formal request to the relevant Force(s) Vetting Unit (regardless of whether that force area was identified on the applicant's documentation) giving relevant details of the trace obtained via INI along with the core details of name, date and place of birth, to facilitate the further search. It is recommended that the relevant record held on INI should be transferred into a 'PDF' or 'word' document and forwarded to the force(s) which holds the information requested.

4.8 The request should be by way of secure email using the generic .pnn police email address system. Use of fax and post should be avoided.

4.9 All forces should create a single vetting email address and vetting single point of contact (SPOC) to receive and coordinate all requests from other forces.

4.10 All material and/or information and/or intelligence to be revealed should be returned to the Force Vetting Unit who made the request. It is the responsibility of the *requesting* force to decide upon the relevance of the information. All material provided must be treated in accordance with the Data Protection Act and the 5x5x5 intelligence grading restrictions (for DPA purposes the force responding to the request remains the Data Controller and therefore, retains legal responsibility for any breaches of DPA relating to any further distribution or disclosure of material provided and therefore, 5x5x5 restrictions must be made clear to the receiving force).

4.11 All forces should respond to the request for information within the ACPO National Vetting Working Group (NVWG) Service Level Agreement of 14 calendar days. The response, and request, should be through the preferred option of secure e-mail as above.

4.12 In addition, if there is any record that another force has, or may have, information or intelligence on that individual, then the existence of such information should be disclosed to the requesting force.

4.13 If through the examination of force records the existence of relatives or associates with information or intelligence held on them is discovered, this should be disclosed to the requesting force.

5. Checks

5.1 Checks must be carried out on all the individuals named on the application form. With regard to non-police personnel, checks must always be made on the applicant and made on the extended family, as appropriate. Vetting enquiries should be conducted in respect of all individuals named on the vetting questionnaires who are over the age of criminal responsibility i.e. 10 years in England and Wales, 8 years in Scotland.

6. Disclosure

6.1 All checks should be recorded and managed and the reply retained by both the sending and receiving force. All information and intelligence passed should be assessed using the National Intelligence Model 5x5x5 system and Data Protection Principles to ensure robust data protection, management and an audit of the exchange of information.

6.2 The 'receivers' of the information are not the 'owners' of the information. Any request for disclosure should be discussed with the 'owning' force as a matter of routine prior to any response. Particular care must be taken when the information relates to intelligence, in this case before disclosure of any information, or existence of such information, contact must be made with the owning force. However, directing the individual towards another force area can in itself highlight the existence of information or intelligence, thus, great care must be taken in matters of this nature. In this case, it is essential that there is a clear, audited dialogue between the forces.

7. Responsibilities

7.1 This SOP is owned by the ACPO Professional Standards Committee.

7.2 Responsibility for implementing and reviewing the Standard Operating Procedure rests with the ACPO National Vetting Working Group.

8. Associated Documents and Policies

- ACPO/ACPOS National Vetting Policy for the Police Community
- Security Policy Framework (SPF)
- Recruitment Vetting SOP 3
- Management Vetting and Enhanced Management Vetting SOP 4
- Non-Police Personnel Vetting SOP 5
- National Security Vetting SOP 6

ACPO Professional Standards Committee

Standard Operating Procedure Number 14

RECIPROCAL VETTING

Protective Marking	NOT PROTECTIVELY MARKED
Publication Scheme Y/N	Yes
Title	Reciprocal Vetting
Version	3.0
Summary	This Standard Operating Procedure supports the ACPO / ACPOS National Vetting Policy for the Police Community
Management	ACPO National Vetting Working Group
Author	Carol Benton [Lancashire], Stewart Finlayson [Strathclyde], Jonathan Gupta [Staffordshire], Bob Lane [Warwickshire], Alan McCawley [MPS]
Date created	August 2010
Review date	August 2011

1. Introduction

1.1 This Standard Operating Procedure (SOP) supports the ACPO/ACPOS National Vetting Policy for the Police Community (NVP) and associated documents and policies.

1.2 This is a new SOP.

2. Application

2.1 This SOP comes into force on 1st August 2010.

3. Purpose

3.1 The purpose of reciprocal vetting is to ensure that everyone working in Force Vetting Units (FVUs) are vetted to an appropriate standard and that, to maintain the confidentiality, integrity and independence of the process, it is conducted by a force other than the parent force.

3.2 In view of the sensitive nature of the work, the ACPO National Vetting Working Group at their meeting of 1 March 2007 agreed that cross force reciprocal vetting should be included as an option within Version 3 of the NVP.

3.3 Forces are recommended to support this initiative for the following reasons:

- The difficulties of conducting enquiries in relation to colleagues, particularly where matters relating to their personal life are revealed and may make it difficult for the working relationship to continue unaffected with members of their immediate team having that knowledge;
- Conducting in-house enquiries on colleagues may render individuals vulnerable to allegations of corruption due to the associations and close working relationships that might develop within a small team;
- Where issues are raised by the vetting process reciprocal vetting will ensure that objective and impartial decisions are made.

3.4 It is recommended that individuals in FVUs be subject to Management Vetting (MV), with Enhanced Management Vetting (EMV) and Security Check (SC) clearance also where appropriate.

4. Process

Note: 'parent' force refers to the force requesting that vetting be undertaken whilst 'partner' force refers to the force conducting the vetting checks.

4.1 The sponsor within the parent force should notify the partner force that a potential new appointee requires vetting and provide basic contact and post details.

4.2 The partner FVU should issue the relevant forms to the subject for completion.

4.3 The individual should complete the relevant forms and return them under confidential cover direct to the partner FVU. Forces entering in to reciprocal vetting must decide and agree between themselves the arrangements for

conducting the necessary Management Vetting and Enhanced Management checks prior to vetting activity commencing.

4.4 The partner force should initiate enquiries that do not need reference to the parent force, such as Police National Computer (PNC)/Criminal History System (CHS) and financial checks.

4.5 The partner force should initiate those enquiries required from the parent force, such as intelligence checks, special branch, company records as appropriate. The parent force should process the required checks and return the results direct to the partner FVU.

4.6 The partner FVU should prepare a vetting summary and submit it to the partner Force Vetting Officer (FVO) with copies of all traces for decision.

4.7 The partner FVO should make a recommendation to the parent force in the manner agreed by them at the start of the process. Where the recommendation is to withhold clearance, all information must be passed to the parent force to enable an informed decision to be made. Forces entering in to reciprocal vetting process must clearly agree and document their agreed process in this respect prior to vetting activity commencing.

4.8 Since the final decision rests with the parent force, they also hold responsibility for aftercare arrangements and review and/or appeal procedures.

5. Responsibilities

5.1 This SOP is owned by the ACPO Professional Standards Committee.

5.2 Responsibility for implementing and reviewing the SOP rests with the ACPO National Vetting Working Group.

6. Associated Documents and Policies

- ACPO/ACPOS National Vetting Policy for the Police Community
- Security Policy Framework (SPF)
- Management Vetting and Enhanced Management Vetting SOP 4
- National Security Vetting SOP 6

ACPO Professional Standards Committee

Standard Operating Procedure Number 15

Business Interests and Secondary Working

Protective Marking	NOT PROTECTIVELY MARKED
Publication Scheme Y/N	Yes
Title	Business Interests and Secondary Working
Version	3.0
Summary	This Standard Operating Procedure supports the ACPO / ACPOS National Vetting Policy for the Police Community
Management	ACPO National Vetting Working Group
Author	Carol Benton [Lancs], Stewart Finlayson [S'clyde], Jonathan Gupta [Staffs], Bob Lane [Warwicks], Alan McCawley [MPS]
Date created	August 2010
Review date	August 2011

1. Introduction

1.1 This Standard Operating Procedure (SOP) supports the ACPO/ACPOS National Vetting Policy for the Police Community (NVP) and associated documents and policies.

1.2 This is a new SOP

2. Application

2.1 This SOP comes into force on 1st August 2010.

2.2 This procedure applies to the following levels of clearance:

- Recruitment Vetting (RV)
- Management Vetting (MV)
- Enhanced Management Vetting (EMV)
- Security Check (SC)
- Developed Vetting (DV)

3. Purpose

3.1 The purpose of this procedure is to ensure that, where relevant, Force Vetting Units (FVUs) are made aware of business interests/secondary working.

4. Process

4.1 Each force should have its own policy relating to secondary working and business interests for police officers, police staff and members of the Special Constabulary. The policy should be owned by either force Human Resources Departments or Professional Standards Departments.

4.2 Management of Business Interests is not a vetting function.

4.3 In accordance with each force's procedures, it is the responsibility of the designated authority for that force (HR or Professional Standards) to assess the nature of the business interest/secondary employment. In reaching the decision, they should consider whether there is the potential for any prejudicial effect on the individual's suitability to maintain the relevant level of clearance. In certain cases, advice should be sought from the Force Vetting Officer (FVO).

4.4 It is not possible to provide a definitive list of factors which should be taken into consideration when making such a decision, however, the following are examples of factors which may be of relevance:

- Nature of the business interest/secondary employment;
- Potential for a conflict of interest between the individual's role within the force and the business interest/secondary employment;
- Potential for the business interest/secondary employment to lead to future financial difficulties for the individual;
- Whether or not the business interest/secondary employment will require the individual to associate with known criminals/persons of interest.

4.5 Each case must be decided on its individual merits, taking all relevant information into consideration.

4.6 Where an individual's application is granted, they should be reminded that they are under an obligation to notify the relevant authority for that force of **any** *significant change in circumstances*.

5. Responsibilities

5.1 This SOP is owned by the ACPO Professional Standards Committee.

5.2 Responsibility for implementing and reviewing the SOP rests with the ACPO National Vetting Working Group.

6. Associated Documents and Policies

- ACPO / ACPOS National Vetting Policy for the Police Community
- Security Policy Framework (SPF)
- Recruitment Vetting SOP 3
- Management Vetting and Enhanced Management Vetting SOP 4
- National Security Vetting SOP 6

ACPO Professional Standards Committee

Standard Operating Procedure Number 16

Risk Assessment – Third Party

Protective Marking	NOT PROTECTIVELY MARKED
Publication Scheme Y/N	Yes
Title	Risk Assessment – Third Party
Version	3.0
Summary	This Standard Operating Procedure supports the ACPO / ACPOS National Vetting Policy for the Police Community
Management	ACPO National Vetting Working Group
Author	Carol Benton [Lancashire], Stewart Finlayson [Strathclyde], Jonathan Gupta [Staffordshire], Bob Lane [Warwickshire], Alan McCawley [MPS]
Date created	August 2010
Review date	August 2011

1. Introduction

1.1 This Standard Operating Procedure (SOP) supports the ACPO/ACPOS National Vetting Policy for the Police Community (NVP) and associated documents and policies.

1.2 This is a new SOP.

2. Application

2.1 This SOP comes into force on 1st August 2010.

2.2 This SOP should be used where adverse information is revealed on third parties relevant to a vetting clearance.

3. Purpose

3.1 The purpose of this SOP is to assist with the documentation of the decision making process where adverse information is revealed on third parties during the vetting process. It is recognised that there will be occasions where an individual who applies for vetting clearance is associated with those about whom adverse information is held. The risk assessment procedure outlined below will enable any potential risk posed by this to be assessed and therefore a reasoned explanation behind the decision whether or not to grant clearance to the applicant can be maintained.

4. Process

4.1 Where adverse information relating to a third party is revealed, consideration must be given to what risk this information poses to:

a) the organisation;
b) the individual;
c) the public.

Third Party

4.2 A third party is any individual whose details have been supplied as part of the vetting process, or about whom information has been uncovered as part of enquiries undertaken during the vetting process. Examples of third parties include, but are not limited to:

- Parents;
- Partners;
- Siblings;
- Children;
- Extended family;
- Partner's extended family;
- Co-habitant;
- Business partners;
- Known associates.

4.3 Whilst a definitive list of factors which should be taken into consideration cannot be made, the following are factors which may count in support of / against granting clearance.

Factors Against Clearance Being Granted

- Evidence of joint enterprise;
- Currency of convictions / cautions of the third party;
- Currency of intelligence relating to third party;
- Gravity of offences committed by third party;
- Nature of relationship;
- Fiduciary relationship between parties.

Factors in Support of Clearance Being Granted

- Evidence of distance between applicant and third party;
- Currency of convictions / cautions of third party;
- Currency of intelligence relating to third party;
- Gravity of offences committed my third party;
- Openness of applicant;
- Ignorance of third party's activity.

4.4 The factors listed above should only be used as a guide as to what kind of information should be taken into consideration. It is stressed that **each case must be decided on its own merits**, taking all relevant information into account.

4.5 Where a decision is made to grant clearance following a risk assessment, safeguards should be put in place to minimise the risk posed. These may include:

a) Management Intervention – close line management supervision may be recommended if the risk assessment shows that there is the potential for a conflict of interests;
b) Ethical Interview – it is advised that, where practicable, an ethical interview should be conducted with the applicant to ascertain the exact nature of their relationship with the third party and also to ascertain what level of knowledge they have of the third party's activity;
c) Disclosure – in extreme cases, it may be pertinent to disclose the information relating to the third party to the applicant. However, it is recommended that such a decision should only be made at Executive level, having considered all ramifications, including legislative restraints, such as the Data Protection Act.

4.6 Where RV clearance is granted to an individual who has known risks and / or vulnerabilities associated to them, sanctions cannot be made against them at a later date on the basis of these known issues.

4.7 Where the applicant has omitted the declaring of an individual whose details are required on vetting forms and adverse information is held about that individual, the assumption should be that the details have been deliberately omitted and should ordinarily be treated as an integrity issue in the first instance.

5. Responsibilities

5.1 This SOP is owned by the ACPO Professional Standards Committee.

5.2 Responsibility for implementing and reviewing the SOP rests with the ACPO National Vetting Working Group.

6. Associated Documents and Policies

- ACPO/ACPOS National Vetting Policy for the Police Community
- Security Policy Framework (SPF)
- Recruitment Vetting SOP 3
- Management Vetting and Enhanced Management Vetting SOP 4
- Non-Police Personnel Vetting SOP 5
- National Security Vetting SOP 6
- Vetting Interviews SOP 7

ACPO Professional Standards Committee

Standard Operating Procedure Number 17

Adverse Information and Judicial Findings (TAINT)

Protective Marking	NOT PROTECTIVELY MARKED
Publication Scheme Y/N	Yes
Title	Adverse Information and Judicial Findings (TAINT)
Version	3.0
Summary	This Standard Operating Procedure supports the ACPO / ACPOS National Vetting Policy for the Police Community
Management	ACPO National Vetting Working Group
Author	Carol Benton [Lancashire], Stewart Finlayson [Strathclyde], Jonathan Gupta [Staffordshire], Bob Lane [Warwickshire], Alan McCawley [MPS]
Date created	August 2010
Review date	August 2011

1. Introduction

1.1 This Standard Operating Procedure (SOP) supports the ACPO / ACPOS National Vetting Policy for the Police Community (NVP) and associated documents and policies.

1.2 This is a new SOP

2. Application

2.1 This SOP comes into force on XXXXX.

3. Purpose

3.1 The purpose of this SOP is to ensure that issues relating to taint are taken into consideration when determining whether vetting clearance should be granted or not.

3.2 The principles of taint are set out in Chapter 18 of the Crown Prosecution Service (CPS) Prosecution Team Disclosure Manual (previously the Joint Operational Instructions – JOPI).

3.3 The driver for the implementation of taint is best demonstrated through case law.

3.4 ***R v Edwards*** ***(1991)*** – This case was an appeal against a conviction for armed robbery. The SIO had been the subject of a disciplinary reprimand for forging interview notes in a previous case. This was not disclosed to the defence in the original trial. The appeal was allowed and the conviction quashed.

3.5 ***R v Guney*** ***(1998)*** – This was an appeal against a conviction for possession of drugs and firearms. A number of officers involved in the original arrest & investigation had been investigated under Operation JACKPOT (an internal misconduct investigation). Details of Operation JACKPOT had not been disclosed to the defence in the original trial. Again, the appeal was allowed.

3.6 In the above case, the following judicial comment was made:
"Evidence of previous misconduct may help demonstrate that the weight to be attached to the evidence of a witness is limited or derisory".

4. Process

4.1 When a Police Officer, Special Constable or member of Police Staff is required to give evidence at Court in England and Wales in their official capacity, they are required to complete a form MG6B, disclosing relevant information, such as:

- Details of any criminal convictions/cautions, spent or otherwise and penalty notices;
- Details of any criminal offences for which summons have yet to be issued;
- Details of any criminal proceedings which have not been completed;
- Details of any adverse Judicial Findings or comment in a criminal or civil court that the individual has misled the court;

- Details of Police discipline (including Police Staff)
  - Disciplinary findings of guilt at a misconduct tribunal
  - Relevant formal written warnings and relevant disciplinary cautions
  - Disciplinary proceedings which have not been completed.

4.2 Any information disclosed is evaluated by the CPS and may be forwarded to the defence.

4.3 It is therefore of the utmost importance that those whose evidence cannot be relied upon in Court are not recruited to police forces.

4.4 It should be borne in mind that there are anomalies between taint and National Police Improvement Agency (NPIA) Circular 01/2010.

4.5 Under the above circular, it would be possible for a tainted individual to be appointed as a Police Officer.

4.6 When considering applications for RV clearance the ramifications of historic convictions/cautions for certain offences, such as those involving deception/violence, should be evaluated in light of the requirements of Chapter 18 of the CPS Disclosure Manual i.e. such offences which would always be disclosed to the CPS.

4.7 The impact of appointing an individual who is tainted cannot be underestimated and can heavily affect the deployment of such an individual on appointment, and in some cases throughout their career. Generally, the impact of taint will lessen as the time since the 'finding' recedes. Thus, when recruiting or appointing a tainted individual, they must be made aware of the impact that such a requirement will have on their career. Particular care must, therefore, be taken when clearing a candidate who will have to disclose matters outlined in paragraph 4.1.

4.8 Further guidance can be obtained from the CPS Prosecution Team Disclosure Manual, Chapter 18.

5. Scotland

5.1 A joint protocol exists in Scotland between the Scottish Police Service and the Crown Office and Procurator Fiscal Service (COPFS). A service wide agreement sets out business rules for the disclosure to the defence of statements, previous convictions and outstanding charges.

5.2 In Scotland, previous convictions and outstanding charges are recorded on the Criminal History System (CHS) and a CHS number is allocated to the person who is the subject of such a record.

5.3 Scottish police forces carry out regular checks and details of all Police Officers in Scotland with CHS numbers are sent to the COPFS and entered on a secure database. Prior to any trial a search of the database is made by COPFS to ascertain if any of the police witnesses are recorded. The decision to disclose convictions or outstanding previous charges is at the discretion of COPFS and is dependent on a number of matters.

5.4 At present the process only applies to police officers.

6. Responsibilities

6.1 This SOP is owned by the ACPO Professional Standards Committee.

6.2 Responsibility for implementing and reviewing the SOP rests with the ACPO National Vetting Working Group.

7. Associated Documents and Policies

- ACPO / ACPOS National Vetting Policy for the Police Community
- Crown Prosecution Service (CPS) Prosecution Team Disclosure Manual
- NPIA Circular 01/2010
- Recruitment Vetting SOP 3

ACPO Professional Standards Committee

Standard Operating Procedure Number 18
FINANCIAL VETTING

Protective Marking	NOT PROTECTIVELY MARKED
Publication Scheme Y/N	Yes
Title	Financial Vetting
Version	3.0
Summary	This Standard Operating Procedure supports the ACPO / ACPOS National Vetting Policy for the Police Community
Management	ACPO National Vetting Working Group
Author	Carol Benton [Lancs], Stewart Finlayson [S'clyde], Jonathan Gupta [Staffs], Bob Lane [Warwicks], Alan McCawley [MPS]
Date created	August 2010
Review date	August 2011

1. Introduction

1.1 This Standard Operating Procedure (SOP) supports the ACPO / ACPOS National Vetting Policy for the Police Community (NVP) and associated documents and policies.

1.2 This is a new SOP.

2. Application

2.1 This SOP comes into force on 1st August 2010.

2.2 This SOP applies to all applicants who are required to undergo financial checks for either force vetting or national security vetting purposes.

3. Purpose

3.1 All members of the police service are in a privileged position with regard to access to information and could be considered potentially vulnerable to corruption.

3.2 The purpose of conducting financial checks is to meet the force's obligations in respect of the prevention of crime and public safety by assessing applicants' financial position, either at the point of entry in to the organisation or as they apply to move into sensitive or 'designated' posts.

4. Process

Force Vetting

Recruitment Vetting

4.1 National Police Improvement Agency (NPIA) Circular 01/2010 states that applicants to the police service should normally be free from undischarged debt or liability and be able to manage existing loans. The emphasis should be on the sensible management of debt.

4.2 ACPO National Vetting Policy Version 1 recommended that the same standards be applied to applicants for police staff roles.

4.3 Paragraph 4 of Schedule 1 to the Police Regulations 2003 states that a member of a police force shall not wilfully refuse or neglect to discharge any lawful debt. This applies to Police Officers and Members of the Special Constabulary only, not Police Staff.

4.4 Application and/or vetting forms will include a number of finance related questions and the security vetting process should include a check with a credit reference agency.

4.5 Applicants who have existing County Court / Sheriff Court Judgements outstanding against them should not be considered.

4.6 Applicants who have discharged the County Court Judgements / Sheriff Court Judgements should be considered.

4.7 Applicants who are subject of a current Individual Voluntary Arrangement (IVA) / Trust Deed should not be considered.

4.8 Applicants who have discharged the IVA / Trust Deed should be considered.

4.9 Applicants who have been registered bankrupt / subject of sequestration and their bankruptcy / sequestration debts have not been discharged should not be considered.

4.10 Applicants who have been registered as bankrupt / subject of sequestration and their bankruptcy / sequestration debts have been discharged should not be considered until three years after the discharge of the debt.

4.11 For the purposes of police recruitment, former Directors of limited companies which have become insolvent who apply to the police force should be treated as if he/she were bankrupt even though the debts are in the name of the company.

4.12 Careful consideration should be given where a credit reference check reveals that applicants have defaulted account(s).

4.13 Where debts are declared, the financial vetting check should be made at the start of the recruitment process. Otherwise, it may be conducted post assessment and prior to appointment.

Non-Police Personnel Vetting (NPPV)

4.14 Financial checks are required for NPPV Levels 2 and 3 and the above principles should be applied (see SOP 5).

Management Vetting (MV)

4.15 The purpose of MV is to provide a means of ensuring that persons serving in 'designated' posts, with access to sensitive police information, intelligence, financial or operational assets, have been assessed as to their reliability and integrity.

4.16 During the course of the vetting process applicants' are asked to provide details about their financial circumstances. This information is checked against a credit reference agency. As individuals are most vulnerable when they have large debts which they cannot sustain, the purpose of financial enquiries is to ensure they have direct or indirect access to sufficient funds to minimise the risk of vulnerability to financial inducement. Where anomalies are noted between their declaration and the information provided by the credit check or where there is a need to clarify a particular issue, individuals will be interviewed.

4.17 When financial information has been provided 'in confidence' as part of the vetting process the risk of compromise is significantly reduced. Applicants should be re-assured that there is no need to be concerned about mortgage and credit card commitments that are in line with their income, providing they have the ability and will to meet the commitments. Debts only become a problem where they are substantial and individuals in 'designated' posts fail to take remedial action or where they are caused by compulsive behaviour e.g. gambling. Debts notified during the process will be dealt with in confidence and from a welfare perspective.

4.18 Where financial problems are identified during the vetting process the Force Vetting Officer (FVO) will discuss the issue with the applicant and will, where possible, rather than refuse vetting clearance, seek to manage the problem within the workplace through welfare support or by discussing the issue with the relevant line manager, with the agreement of the applicant. If the applicant refuses to consent to such a 'management' process then MV clearance is unlikely to be granted.

4.19 If a line manager becomes aware that an individual serving in a 'designated' post has financial difficulties then they should explore the issue with them and seek welfare intervention at an early stage. The FVO should also be advised.

National Security Vetting

4.20 The current policy for national security vetting is contained within the Cabinet Office' Security Policy Framework and details can also be found in National Security Vetting SOP 6. Financial checks form part of the Security Check (SC) and Developed Vetting (DV) processes.

4.21 ACPO(S) Vetting Policy states that it is only when applicants for SC or DV clearance have received MV clearance that the additional SC checks should be carried out. Thus the financial vetting check will be carried out as part of the MV process.

5. Responsibilities

5.1 This SOP is owned by the ACPO Professional Standards Committee.

5.2 Responsibility for implementing and reviewing the SOP rests with the ACPO National Vetting Working Group.

Associated Documents and Policies

- ACPO / ACPOS National Vetting Policy for the Police Community
- Security Policy Framework (SPF)
- NPIA Circular 01/2010
- Police Regulations 2003
- Recruitment Vetting SOP 3
- Management Vetting and Enhanced Management Vetting SOP 4
- Non-Police Personnel Vetting SOP 5
- National Security Vetting SOP 6

ACPO Professional Standards Committee

Standard Operation Procedure Number 19

GLOSSARY OF TERMS AND ABBREVIATIONS

Protective Marking	NOT PROTECTIVELY MARKED
Publication Scheme Y/N	Yes
Title	Glossary of Terms and Abbreviations
Version	3.0
Summary	This Standard Operating Procedure supports the ACPO / ACPOS National Vetting Policy for the Police Community
Management	ACPO National Vetting Working Group
Author	Carol Benton [Lancashire], Stewart Finlayson [Strathclyde], Jonathan Gupta [Staffordshire], Bob Lane [Warwickshire], Alan McCawley [MPS]
Date created	August 2010
Review date	August 2011

1. Introduction

1.1 This Standard Operating Procedure (SOP) supports the ACPO / ACPOS National Vetting Policy for the Police Community (NVP) and associated documents and policies.

1.2 This is a new SOP.

2. Application

2.1 This SOP comes into force on 1st August 2010.

3. Glossary of Terms

ACPO	Association of Chief Police Officers
ACPOS	Association of Chief Police Officers in Scotland
ARC	Application Registration Card
BC	Basic Check
BS	Baseline Standard
CHS	Criminal History System
CIS	Criminal Intelligence System
CRC	Credit Reference Check
CSA	Customer Supplier Agreement
CTC	Counter Terrorist Check
DPA	Data Protection Act 1998
DSO	Home Office Departmental Security Officer
DV	Developed Vetting
DVA	Defence Vetting Agency
DWP	Department of Work and Pensions
ECHR	European Convention Human Rights
EEA	European Economic Area
EIA	Equality Impact Assessment
EMV	Enhanced Management Vetting

FMO	Force Medical Officer
FSM	Force Security Manager
FSO	Force Support Officer
FVO	Force Vetting Officer
FVOAG	Force Vetting Officers Advisory Group
GPMS	Government Protective Marking Scheme
HMG	Her Majesty's Government
HMIC	HM Inspectors of Constabulary
HMRC	Her Majesty's Revenue and Customs
HOC	Home Office Circular
HSB	Head of Special Branch
IAG	Independent Advisory Group
INI	IMPACT Nominal Index
ISA	Independent Safeguarding Authority
LIO	Local Intelligence Office(r)
MV	Management Vetting
MOD	Ministry of Defence
MoPS	Manual of Protective Security (now replaced see SPF)
NPIA	National Police Improvement Agency
NPPV	Non-Police Personnel Vetting
NSV	National Security Vetting
NVWG	National Vetting Working Group
PCSO	Police Community Support Officer
PNC	Police National Computer
PSC	Professional Standards Committee
RV	Recruitment Vetting
SB	Special Branch
SC	Security Check Vetting

SCRO	Scottish Criminal Records Office
SOP	Standard Operating Procedure
SPF	Security Policy Framework (Previously MoPS)
STRAP	Handling regime for the most sensitive of Security and Intelligence Assets
SVAP	Security Vetting Appeals Panel
.gsi	Government Secure Intranet

4. Responsibilities

4.1 This SOP is owned by the ACPO Professional Standards Committee.

4.2 Responsibility for implementing and reviewing the Standard Operating Procedure rests with the ACPO National Vetting Working Group.

5. Associated Documents and Policies

- ACPO / ACPOS National Vetting Policy for the Police Community
- Security Policy Framework (SPF)
- NPIA Circular 01/2010