Service Instruction 0818
Personnel Security

Document Control

Description and Purpose

This document is intended to ensure compliance with the requirements of Her Majesty's Government's (HMG) Security Policy Framework and to safeguard Authority information and assets

Active date	Review date	Author	Editor	Publisher
28.02.14	28.02.15	Vicky Walsh	Suzanne Lea	Sue Coker

Permanent	X	Temporary		If temporary, review date must be 3 months or less.

Amendment History

Version	Date	Reasons for Change	Amended by
1.0	11.03.14	Update to information on draft version	Deb Appleton

Risk Assessment (if applicable)

Date Completed	Review Date	Assessed by	Document location	Verified by(H&S)

Equalities Impact Assessment

Initial	Full	Date	Reviewed by	Document location
	X	21.01.14	Wendy Kenyon	Strategy & Performance/EIA's/Approved for Publish 2014

Civil Contingencies Impact Assessment (if applicable)

Date	Assessed by	Document location

Related Documents

Doc. Type	Ref. No.	Title	Document location
Policy	STRPOL14	Protective Security	TBC
Policy	TBC	Recruitment & Selection	TBC
Policy	STRPOL09	Information Governance & Security	Portal
Instruction	SI 0816	Protective Marking – Government Security Classifications and Government Protective Marking Scheme	
Instruction	SI 0759	Destruction of information Assets Including Protectively Marked Information	Portal
Instruction	SI 0435	Data Protection Instructions	Portal
Instruction	SI 0718	Security of Premises and Terrorist Threats	Portal

Contact

Department	Email	Telephone ext.
People & Organisational Development	Contracts&PolicyTeam@merseyfire.gov.uk	0151 296 4360

Target audience

All MFS	x	Ops Crews		Fire safety		Community FS			
Principal officers		Senior officers		Non uniformed					

Relevant legislation (if any)

Data Protection Act (DPA) (1998)
Employment Rights Act (1996)
Equality Act (2010)
Human Rights Act (1998)
Immigration Asylum and Nationality Act (2006)
Rehabilitation of Offenders Act (1974) and the Rehabilitation of Offenders (Northern Ireland) Order (1974)
Trade Union Reform and Employment Rights Act (1993)

INTRODUCTION

The aim of this document is to ensure compliance with the requirements of Her Majesty's Government's (HMG) Security Policy Framework and to safeguard Authority information and assets.

Personnel Security provides a level of assurance as to the trustworthiness, integrity and reliability of all Authority staff. As a minimum requirement all staff will be subject to recruitment controls known as baseline personnel security standard.

For more sensitive posts there is a range of security controls referred to as 'National Security Vetting'; these are specifically designed to ensure that such posts are filled by individuals who are unlikely to be susceptible, for whatever reason or motive, to influence or pressure which might cause them to abuse their position.

These controls "whilst ensuring a degree of risk management" do not provide a guarantee of reliability and must be supported by continuous and effective line management and aftercare arrangements.

Purpose

The purpose of Personnel Security is to provide an acceptable level of assurance as to the integrity of all Authority staff and contractors who are to be given authorised access to buildings, information or other assets belonging to or entrusted to the Authority including the Joint Control Centre. This service instruction aims to ensure that individuals, who need access to such assets in order to carry out their roles, are less likely to be susceptible, for whatever reason or motive, to temptation or pressure that could cause them to abuse the access they have been given.

Review

This policy will be reviewed periodically to ensure uniformity of treatment and justice for all employees in the implementation of the Authority's procedures and to ensure compliance with relevant legislation.

Equality and diversity

Employees must ensure that they treat other employees, Members, Service users and other people with whom they come into contact during their work in a way that complies fully with the Equality Act 2010 and does not discriminate against individuals or groups on the grounds of any protected characteristics.

Applicability

This service instruction will apply to all existing Authority staff, prospective employees, contractors, volunteers and any other similar organisations and will also incorporate the Authority's **Recruitment and Selection policy**.

For the purposes of this procedure the definition of Authority staff applies to:

- substantive
- fixed term
- Part time/full time
- Secondees
- Agency staff
- Work experience/placements

*Please note this list is not exhaustive

General principles

- Before any individual can start employment with the Authority or work on Authority premises, the appropriate level of personnel security must be granted. All candidates must go through a basic disclosure and, dependent upon their role and location, may also go through Police Vetting and/or National Security Vetting.
- Personnel security is a pre-requisite for employment and therefore those who refuse to support the process will not be considered.
- The level of personnel security will be determined by the requirements of the role and will take into account the extent to which unsupervised access to premises, personnel, computer systems and data is required.
- Should an employee change location or role then the appropriate level of personnel security must be granted prior to commencement.

Personnel security risk assessment

In order to rationalise what security controls might be appropriate for particular posts within the Authority, a risk assessment will be conducted. The risk assessment will consider the operating environment of the site, the level of access available to post holders and the potential risk those posts pose to sensitive material, valuable assets and operational capability. Such an assessment will ensure that any proposed security controls, such as the level of screening applied to certain posts, is proportionate and appropriate.

Levels of personnel security screening

There are three levels of personnel security screening within the Authority.

1. Baseline Personnel Security Standard (BPSS)
2. Non-Police Personnel Vetting Level Three (NPPV3)
3. National Security Vetting (NSV) – 3 levels
    a. Counter Terrorism Check (CTC)
    b. Security Check (SC)
    c. Developed Vetted (DV)

General roles and positions

The table below reflects the general roles and positions that are pre-determined generically as requiring particular security controls within the Authority.

Role	Security Control
All Authority staff, prospective employees, contractors, FireFit HUB, Fire Support Network (FSN) and any other similar organisations unless they are required to have NPPV3 for their role which supersedes BPSS	Baseline Personnel Security Standard (BPSS)
All Authority staff, prospective employees, contractors, volunteers and any other similar organisations that require as part of their role or location of work to have access to the Joint Control Centre.	Non-Police Personnel Vetting Level Three (NPPV3)
Brigade Manager	Security Check (SC)
CBRN Silver/Gold Commander	Security Check (SC)
National Interagency Liaison Officer (NILO)	Security Check (SC)
National Resilience Assurance Team	Security Check (SC)

*Please note this list is not exhaustive.

1. BASELINE PERSONNEL SECURITY SCREENING (BPSS)

The Baseline Personnel Security Standard provides a sensible, and in the case of National Security Vetting essential, grounding for making informed employment decisions. The majority of the checks conducted to form a Baseline Personnel Security Standard are mandated by law, such as the confirmation of Nationality and Immigration status.

Those who are cleared to Baseline Personnel Security Standard level may have frequent access up to CONFIDENTIAL, and occasional controlled access to SECRET material as defined in the Government Protective Marking System.

The Baseline Personnel Security Standard is not a formal security clearance within National Security Vetting, but is designed to provide a level of assurance as to the trustworthiness and integrity of individuals whose work, in the main, involves uncontrolled access to, or knowledge or custody of, assets protectively marked up to CONFIDENTIAL.

Baseline Personnel Security Standard is carried out within the Authority as part of the recruitment process. The Baseline Personnel Security Standard comprises verification of four main elements:

- Identity
- Employment history
- Nationality and immigration status
- Unspent criminal record

Procedure for the Verification of Unspent Criminal Records

Basic Disclosure

Verification of unspent criminal records will be undertaken in the form of a basic disclosure. A basic disclosure is a document containing impartial and confidential criminal history information held by the police and government departments which can be used by employers to make safer recruitment decisions.

Cost

The Authority will cover the cost of a basic disclosure required for all Authority staff and prospective employees.

Basic Disclosure Application Form

The basic disclosure application form and guidance notes are available from the Resourcing team, People and Organisational Development Department (POD).

Supporting Documents

Applicants will be required to show two documents to verify their identity and current address to the Resourcing Team, POD on submission of a basic disclosure application form. These could be:

- A passport, driving licence or birth certificate which shows your date of birth (photographic ID is preferred)
- A utility bill, bank, mortgage or credit card statement that shows your address and should be dated within the last 3 months.

Please note that copies of these documents will be posted with the paper application form, to Disclosure Scotland.

Requests for Further Information

Whilst processing the application, Disclosure Scotland may contact the applicant if further information is required. This information must be provided promptly. Any delay in providing this information may result in the withdrawal of any conditional offer of employment.

Receiving the Disclosure Information

The final disclosure certificate following the application process can be sent direct to either the applicant's home address or the Authority, from Disclosure Scotland. If the disclosure certificate is sent direct to the Authority, this must be upon the consent of the applicant.

If the applicant chooses to have the disclosure certificate sent direct to their home they will be required to show the Authority their original disclosure certificate upon receipt. The Authority will sight this document and obtain a copy for recruitment purposes.

No offer of employment or start date with the Authority will be confirmed until a satisfactory basic disclosure certificate has been sighted.

Reviewing the Result of the Disclosure

POD will assess the content of the Disclosure. Any information received will be considered in line with the duties of the post to which you have been conditionally offered.

Satisfactory Disclosure

If a disclosure is considered to be satisfactory, the applicant will have met this condition of appointment and will receive no further correspondence from the Authority about this matter.

Disclosure which requires further review

Where the Disclosure confirms details of unspent convictions, this will not lead to an automatic bar from appointment. POD will review the contents of the Disclosure in line with the requirements of the vacancy and will consider any other information which the applicant has provided regarding their case. As part of this review the applicant may be invited to discuss their case further with a POD manager (appropriate managerial representatives from the recruiting department may also be involved) before a final decision on suitability is made.

All aspects of the review of the Disclosure will be in line with the Authority's Policy Statement on **the Recruitment and Employment of Ex-offenders** attached as **Appendix A** and **Equal Opportunities Policy** available on the Authority's internal portal.

If the individual's circumstances are not compatible with the post, the Authority may be required to withdraw the offer of appointment and will inform all appropriate parties of this outcome.

Management of Information

All documentation relating to the Disclosure application process will be considered highly confidential by all parties involved and will be stored securely by POD, separately from your personal file. Access to documents, and the results of the Disclosure, will be restricted to those who require access as part of their duties, as determined by POD. Documents will only be retained for a reasonable period following which they will be destroyed as confidential material in line with DBS guidance.

Further details are available in the Authority's Policy Statement on the **Secure Handling, Use, Storage, Retention and Destruction of Disclosure Information** attached as **Appendix B**.

Aftercare

In order to ensure ongoing assurance of certain sensitive posts individuals may be required to engage in an annual security appraisal with their line manager.

2. Non-Police Personnel Vetting Level Three (NPPV3)

The NPPV3 level police check is required for any individuals who as part of their role or location of work are required to access the Joint Control Centre or any similar location where MFRS is working in partnership with the police.

This is required by the Merseyside Police to maintain a high standard, preserve the integrity of the force, safeguard assets, gain the trust of the public and deter corrupt/inappropriate behaviour.

Procedure

The checks conducted include:

- Police National Computer check (PNC)
- Intelligence databases including special branch
- Voters register
- Vetting database
- Credit reference
- Secured Network Services (SNS)

Cost

There is no financial impact for the employee.

Application form

The application form is available from the Resourcing team, People and Organisational Development (POD)

Requests for further information

Whilst processing the application, Merseyside Police may contact the applicant if further information is required. This information must be provided promptly. At this stage MFRS are not included in the communications between the Police and the individual.

Decision

The result will be provided to the Resourcing Team who will then forward to the applicant. Merseyside Police will then issue an access card. Unless there is an organisational need this process will renew after 10 years.

Adverse NPPV3 decisions & appeals

If the application is rejected, the individual does have the right of appeal. In the first instance the individual should contact **force.vetting.unit@merseyside.pnn.police.uk**. If clearance is denied, individuals will be informed of the reason on request and this will be provided unless the reason:-

- Damages National Security
- Frustrates the prevention/detection of crime
- Results in the disclosure of sensitive information
- Breaches confidentiality of any information provided in confidence
- Impedes the apprehension or prosecution of offenders.
- Results in the force breaking the law

If the individual wishes to appeal, it is the individual's responsibility to make the appeal direct to the Head of Professional Standards, Merseyside Police and the appeal will be heard in 5 working days.

MFRS – Implications of Rejection

In the case of an employee being rejected by Merseyside Police, the implications will be reviewed by a member of the People & Organisational Development Team on a case by case basis.

Management of Information

All documentation relating to the NPPV3 application process will be considered highly confidential by all parties involved and will be stored securely by POD. Once the application is approved the application form will be destroyed as confidential material in line with the **SI 0759 Destruction of Information Assets including protectively marked information.**

3. NATIONAL SECURITY VETTING (NSV)

a. Counter Terrorism Check (CTC)

CTC clearance is required for those individuals who are to be employed in 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.

b. Security Check (SC)

Those who are cleared to SC level may have long-term, frequent and uncontrolled access to SECRET assets, and occasional, supervised access to TOP SECRET assets as defined in the Government Protective Marking System.

A Security Check may also be applied to staff that are in a position directly or indirectly to bring about the same degree of damage as those described above or who need access to protectively marked material originating from other countries or international organisations. A Security Check clearance will normally consist of:

- Check against the National Collection of Criminal Records and relevant service and police records;
- Check against Security Service records;
- Credit reference check and, where appropriate, a review of personal finances.
- In some circumstances, further enquiries, including an interview with the subject, may be carried out.

A Security Check clearance should not usually be required for:

- Occasional access to SECRET assets in the normal course of business or during conferences or courses.
- Custody of a small quantity of SECRET assets.
- Entry to an area where SECRET assets are stored.
- Work in areas where SECRET or TOP SECRET information might be overheard.
- Use of equipment capable of handling SECRET information (provided that access controls are in place).
- In these circumstances, the Baseline Personnel Security Standard should usually be sufficient.

c. Developed Vetting (DV)

Those who are cleared to DV level may have long term, frequent and uncontrolled access to TOP SECRET information or assets as defined in the Government Protective Marking System.

This level of clearance may also be applied to people who are in a position directly or indirectly to cause the same degree of damage as those described above and in order to satisfy the requirements for access to protectively marked material originating from other countries and international organisations. In addition to a Security Check, a Developed Vetted will involve:

- An interview with the person being vetted;
- References from people who are familiar with the person's character in both the home and work environment. These may be followed up by interviews.

Enquiries will not necessary be confined to past and present employers and nominated character referees.

NSV Procedure (a, b and c above)

Stage 1

If after a thorough risk assessment a post is deemed as requiring a level of NSV a formal request from the post holders line manager detailing the reasons for this request must be sent to **Contracts&PolicyTeam@merseyfire.gov.uk.** Subsequently, The Department for Communities & Local Government (DCLG) will be contacted to commence the vetting process.
DCLG is the Government Sector Sponsor Department for providing National Security Vetting for the all Fire & Rescue Services, where the requirement for NSV is demonstrable.

Stage 2

The applicant will receive an email direct to their work email address containing guidance sent from the DCLG vetting team. Applicants must read the guidance and complete all relevant parts of the Application for National Security Vetting Clearance form titled 'Annex A'.

The form will request the details of the 'Candidate HR contact details' which the applicant should detail as **Contracts&PolicyTeam@merseyfire.gov.uk**.

Once complete, 'Annex A' should be sent under confidential cover, including wet signatures, to the Vetting Team within POD who will then forward to DCLG by recorded delivery. The applicant must keep a copy of this document for their records and to assist the log in process in stage 3.

If any section of the form is incomplete, the form will not be processed and the sender notified accordingly.

Please note, there are strict deadlines in which stages of the application process have to be completed by. Applicants must adhere to these deadlines. Failure to adhere to these deadlines will have a costly monetary impact for DCLG and may therefore result in a complaint being submitted to the Chief Fire Officer may result in disciplinary action being taken against the applicant as per the Authority's Disciplinary procedure.

Stage 3

If NSV is granted, the Defence Business Services will be notified, who will email the applicant the necessary access to the Cerberus vetting system.

The Vetting Team within POD will also be contacted at this point for further information on the applicant. At this point, the applicant may be requested to provide their original passport to a member of the Vetting Team within POD.

The Defence Business Services and the sponsoring government department will then take responsibility for the remainder of the vetting process.

Duration of application

The duration of a NSV application is dependent on the level of clearance requested and the level of inquiry particular to each application. The length of time between receipt of application and decision on security clearance ranges from 3 weeks to 3 months. The applicant will be notified direct of the outcome in respect of the security clearance decision.

Decision

The decision to grant or decline clearance will be taken by a Government Departmental Security Officer, in collaboration with the Chief Fire & Rescue Adviser (CFRA) Senior Fire & Rescue Security Adviser where necessary. However, before making a final decision, the Departmental Security Officer and/or CFRA Senior Fire & Rescue Security Adviser may ask for additional checks or enquiries to be made, calling the applicant for an interview, or asking for additional referees.

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

Circumstance which may present a risk to security

These factors may justify a decision to refuse, limit or withdraw vetting clearance. The list should not be considered exhaustive:

- Significant financial difficulties or debts.
- Compulsive drinking or gambling.
- Illegal use of controlled or prescribed drugs.
- Other conduct likely to lead to such pressure.
- The likelihood that the applicant's performance of duty will be adversely affected e.g. through adverse pressure or a conflict of interest.
- The nature, number and seriousness of any recorded offences or involvement in criminal activity and the time period within which these took place.
- If the circumstances are likely to bring discredit to the Authority or cause embarrassment.
- If the fact of any conviction will genuinely induce a conflict of interest in the discharge of the applicant's duties.

Commencement of work prior to receipt of NSV

Where there is to be a change in personnel filling a vettable post, it is important to ensure that, as far as is practicable, the new incumbent is cleared before taking up post. Where that is not possible the process should be put underway at the earliest opportunity. In the interim, every effort should be made to ensure that the individual does not have access to material for which they have not been cleared.

Change of circumstances

It is a statutory requirement and an individual's responsibility to report any relevant changes to their circumstances that may impact on the suitability to hold a security clearance to their line manager. This is especially important for those individuals whose roles require NSV at CTC, SC and DV levels.

It is the responsibility of line managers to ensure that the Vetting Team within POD is notified of relevant changes coming to their attention.

Failure to notify your line manager of any changes which might affect security clearance may be subject to disciplinary action as per the Authority's Disciplinary procedure.

Aftercare

Personnel Security controls are based on a 'snapshot in time' and an individual's personal circumstances may be subject to a significant change which may affect their suitability to maintain their clearance.

It is therefore vital that the individual's suitability is assessed through an aftercare regime. This may require checks to be carried out to determine whether the changes represent a potential risk to the integrity of the Authority.

Staff subject to NSV will be contacted by the Vetting Team within POD on an annual basis to undertake a security appraisal. This routine but important process is required for all individuals

cleared to the highest levels in order to review the continued suitability to access highly classified information and assets. The appraisal allows the Authority to update records to reflect any changes to personal circumstance and identify and review any issues that may relate to security

The Authority may need to make follow-up enquiries concerning information provided, particularly where personal circumstances have changed.

Renewal of NSV clearance

A clearance does not last indefinitely therefore individuals whose clearance is due for renewal will be required to complete new questionnaires. The process will be conducted in line with the criteria for initial vetting. Any level of clearance may be renewed at an earlier stage if a higher clearance is required or reviewed if information comes to light relating such as a material change in an employee's personal circumstances.

Leaving a post requiring NSV

Once an individual has left a vettable post, making the clearance requirement redundant, the applicant must advise the Vetting Team within POD who will in turn advise DCLG of this change.

In cases when staff end their employment, their vetting clearance will be revoked. Where they are required to resign as an alternative to dismissal, or are dismissed from the Authority, or resign prior to misconduct hearing, where there are clear concerns about their integrity or ability to hold NSV clearances, the Security Service will be notified immediately.

Adverse NSV decisions & appeals

The appeals procedure for NSV is available to those individuals refused NSV clearance.

Where a National Security Vetting clearance request is refused, or where withdrawal of National Security Vetting clearance has taken place, a process exists that requires an appeal to DCLG. The appeal may result in the original decision to refuse or withdraw clearance being overturned.

Request for an appeal or review must be made in writing, and must be from the applicant themselves, or endorsed by the applicant. The appeal should then be submitted to the DCLG Departmental Security Officer within 10 working days of receiving notification of the refusal/withdrawal.

MFRS – Implications of Rejection

In the case of an employee being rejected following the NSV process, the implications will be reviewed by a member of the People & Organisational Development Team on a case by case basis.

Career breaks & secondments

Individuals on career break or secondment will continue to be regarded as employees of the Authority and remain subject to the Authority's conditions of service.

All individuals who have been on career break or secondment may be required to submit a full vetting application and must provide written declaration indicating whether or not they have come to the attention of the police or relevant Law Enforcement Agencies, through their POD contact prior to their return. The application will be clearly marked indicating the length of time the employee has been on career break or secondment together with the details of any time spent out of the Country.

Retention of NSV records

All papers obtained during the course of the vetting enquiries and utilised in the decision making process, whether clearance is granted or not, will be retained for the period shown below:

- If cleared the papers will be retained for the duration of the clearance.
- 1 year after leaving the Authority.
- 1 year after any vetting clearance is withdrawn.
- 3 years after any vetting clearance is refused.

APPENDIX A

"An Excellent Authority"

POLICY ON THE RECRUITMENT OF EX-OFFENDERS

Policy Statement

1. The Code of Practice ("the Code") is published by the Secretary of State under section 122 of Part V of The Police Act 1997 ("the 1997 Act"). The Code identifies obligations which registered bodies, counter signatories and other recipients of disclosure information issued under the 1997 Act and the Safeguarding of Vulnerable Groups Act ("the 2006 Act").
2. We comply with the Code, the 1997 and 2006 Acts regarding the treatment of individuals who are subject to Disclosure Scotland checks. We undertake not to discriminate unfairly against the subject of a disclosure on the basis of conviction or other information revealed.
3. We will provide a copy of this policy and the Code to anyone who asks to see it.
4. We are committed to equality of opportunity, to following practices, and to providing a service which is free from unfair and unlawful discrimination. We ensure that no applicant or member of staff is subject to less favourable treatment on the grounds of offending background. We actively promote the right mix of talent, skills and potential and welcome applications from a wide range of candidates, including those with criminal records. The selection of candidates for interview will be based on skills, qualifications and experience.
5. We will use a Disclosure Scotland check only where this is considered proportionate and relevant to the particular position or type of regulated work. This will be based on a thorough risk assessment of the position or work and having considered the relevant legislation which determines whether or not a Standard or Enhanced Disclosure under the 1997 Act or a request for disclosure under the 2006 Act is applicable.
6. Where a disclosure application or request is deemed necessary, individuals will be made aware that the position or work will be subject to a Disclosure Scotland check and that the nature of the position or work entitles us to ask about spent and unspent convictions.
7. We will ask individuals to complete a criminal record self-declaration form. We will stress to individuals that they should be honest in their response. We will ask that this form be returned under separate, confidential cover, to a designated person within our organisation and we guarantee that this form will only be seen by those who need to see it as part of the decision-making process.
8. At interview, or under separate discussion, we undertake to ensure an open and measured discussion on the subject of any offences or other matters that might be considered relevant for the position or work concerned.
9. We undertake to discuss any matter revealed in a certificate issued under the 1997 Act or a Scheme Record issued under the 2006 Act with the subject of that disclosure before a decision is made.
10. We ensure that all those who are involved in the decision making process have been suitably trained to identify and assess the relevance and circumstances of disclosure information. We also ensure that they have received appropriate guidance and training about providing work for ex-offenders.

HAVING A CRIMINAL RECORD WILL NOT NECESSARILY DEBAR YOU FROM WORKING WITH US.

1 We are only able to discuss what is contained on a Disclosure Certificate and not what may have been sent under separate cover by a police force.

APPENDIX B

"An Excellent Authority"

POLICY ON THE SECURE HANDLING, USE, STORAGE, RETENTION AND DESTRUCTION OF DISCLOSURE INFORMATION

Note: The Authority has several service instructions relating to information security and governance that may also be relevant. However, in the case of basic disclosure information the process in this appendix must also be followed.

Policy Statement

Introduction

1. The Code of Practice ("the Code") is published by the Secretary of State under section 122 of Part V of The Police Act 1997 ("the 1997 Act"). The Code sets out obligations for registered bodies, counter signatories and other recipients of disclosure information issued under the 1997 Act and the Safeguarding of Vulnerable Groups Act 2006 ("the 2006 Act").

General Principles

2. We comply with the Code and the 1997 and 2006 Acts regarding the handling, holding, storage, destruction and retention of disclosure information provided by Disclosure Scotland. We comply with the Data Protection Act 1998 ("the 1998 Act"). We will provide a copy of this policy to anyone who requests to see it.

Usage

3. We will use disclosure information only for the purpose for which it was requested and provided. Disclosure information will not be used or disclosed in a manner incompatible with that purpose. We will not share disclosure information with a third party unless the subject has given their written consent and has been made aware of the purpose of the sharing.

Handling

4. We recognise that, under section 124 of the 1997 Act it is a criminal offence to disclose disclosure information to any unauthorised person. Disclosure information is only shared with those authorised to see it in the course of their duties. We will not disclose information provided under subsection 113B(5)2 of the 1997 Act, namely information which is not included in the certificate, to the subject.

Access and Storage

5. We do not keep disclosure information on an individual's personnel file. It is kept securely, in lockable, non-portable storage containers. Access to storage units is strictly controlled and is limited to authorised named individuals, who are entitled to see such information in the course of their duties.

Retention

6. To comply with the 1998 Act, we do not keep disclosure information for longer than necessary. For the 1997 Act, this will be the date the relevant decision has been taken, allowing for the resolution of any disputes or complaints. For the 2006 Act, this will be the date an individual ceases to do regulated work for this organisation. We will not retain any paper or electronic image of the disclosure information. We will, however, record the date of issue, the individual's name, the disclosure type and the purpose for which it was requested, the unique reference number of the disclosure and details of our decision. The same conditions relating to secure storage and access apply irrespective of the period of retention.

Disposal

7. We will ensure that disclosure information is destroyed in a secure manner i.e. by shredding, pulping or burning. We will ensure that disclosure information which is awaiting destruction will not be kept in any insecure receptacle (e.g. a waste bin or unlocked desk/cabinet).

Umbrella Bodies

8. Before acting as an Umbrella Body (a body which countersigns applications for Standard or Enhanced Disclosures or makes declarations in relation to PVG disclosure requests on behalf of other organisations) we will take the following steps. We will ensure that the organisation on whose behalf we are acting complies with the Code and the 1997 and 2006 Acts. We will take all reasonable steps to satisfy ourselves that they will handle, use, store, retain and dispose of disclosure information in full accordance with this policy. We will also ensure that anybody or individual for whom applications or requests are countersigned, has such a written policy. If necessary, we will provide a model policy for that body or individual to use or adapt for this purpose.