LONDON FIRE BRIGADE

Personnel security policy

New policy number:	**865**
Old instruction number:	
Issue date:	**27 March 2015**
Reviewed as current:	**24 July 2023**
Owner:	**Assistant Commissioner, Operational Resilience and Control**
Responsible work team:	**Head of Vetting**

Contents

1 Introduction

1.1 This policy sets out the Brigade's arrangements for undertaking higher level vetting and screening checks for staff who occupy security sensitive roles or undertake work, exposing them to information, situations or resources that carry with them a raised level of national security sensitivity.

1.2 As a public sector emergency service, the Brigade needs to operate in a secure manner and maintain appropriate levels of security in work, and exposure to the work of other organisations. To safeguard the people of London, access to information, equipment and property will be maintained at an appropriate level. Therefore adequate staff checks or screenings are required which will be determined by role, the area of work, and any other potential security considerations.

2 Personnel checks

2.1 Personnel checks are carried out on all staff to some level; on all new employees, and for non-employees working as volunteers or in work placements if appropriate.

2.2 Personnel checks are carried out in the following categories;

(a) Employment Disclosure, a basic disclosure of criminal records carried out on all newly recruited staff across all staff groups.

As appropriate a standard or enhanced disclosure of criminal convictions is required, provided it is proportionate and relevant to the position concerned.

(b) National Security Checks are formal security clearances that allow access to more sensitive information, premises or assets.

These may apply to:

- Staff engaged in inter-agency activities or projects, specifically with access to sensitive information requiring security clearance.
- Staff with access to planning or the decision making process which can involve visiting, premises, using resources, or accessing information that could potentially compromise security.

Personnel requiring national security vetting will already have, or may be required to complete a basic criminal record check via the Disclosure and Barring Service as detailed in policy number 0726 - Disclosure and barring policy.

3 Higher level vetting and screening

3.1 Brigade staff confirmed as requiring national security vetting will undergo one of the following categories of vetting:

(a) Non-Police Personnel Vetting Level 2 (NPPVL2): is required for those individuals who require some access to Metropolitan Police buildings. It also permits access to police assets up to the level of 'Official Sensitive', with occasional access to 'Secret assets'.

This level of check will be applied as appropriate to role, or requirements.

(b) Counter Terrorist Check (CTC): is required for those individuals who require regular access to information classified as 'UK OFFICIAL SENSITIVE' ,assets and occasional access to information classified as 'UK SECRET' assets. Or for individuals in a position where there is the potential to directly or indirectly cause the same degree of damage.

(c) Security Check (SC): is required for those individuals who require long term frequent and uncontrolled access to government assets marked 'SECRET'; require occasional supervised access to government assets marked 'TOP SECRET'.

Appointments to; deputy assistant commissioner (DAC) and above, including temporary cover, appropriate Staff Officers, National Inter-Agency Officers (NILO) and senior members of staff from other staff groups will most likely require this (higher level SC) clearance, but can be determined on a case by case basis.

3.2 Vetting clearance will be in place only for as long as it is deemed appropriate in relation to the work an individual undertakes. Clearance can be removed when the nature of the work or role changes. All clearances will cease on the last day of service with the Brigade.

3.3 As specific roles within departments, staff seniority, or exposure to information may require individuals to have a higher level of vetting and screening. At all times, this screening will only be carried out with the agreement of the Brigade's security adviser based in the Special Operations Group (SOG) in the first instance.

4 Process for higher level vetting and screening–current staff

4.1 New requests for higher level vetting and screening must be directed to the Brigade's security adviser in the first instance. The adviser will then request the Vetting Team to instigate the process. Requests that fail to observe this process will be declined.

4.2 The Vetting Team will provide the individual with vetting forms and instructions on how to complete them. Forms must be completed electronically and then emailed back to the HR Services manager for checking.

4.3 Following receipt of the completed form, the individual needs to present the necessary identity documents (originals only) by prior appointment to the Vetting Team. Copies are made of the documents and the electronic forms are printed and signed by both the individual and member of the Vetting Team.

4.4 The electronic forms are then emailed to the Metropolitan Police Service (MPS) for vetting. The paper documents are kept in a secure, locked cabinet and are destroyed when the vetting process is completed.

4.5 The vetting notification is emailed to the Vetting Team by the MPS. Details are recorded on to the Vetting Team system and the paper documents are securely shredded. The individual and the security adviser are informed of outcome.

5 Process for higher level vetting and screening–new staff

5.1 When a position is newly vacant or created, and may require a higher level of vetting and security, it is the line managers responsibility to confer with the Brigade's security adviser to confirm the necessity of a higher level vetting process.

5.2 The successful candidate will have to undergo a basic disclosure in the first instance, as per the Baseline Personnel Security Standards if not already undertaken.

5.3 Once received, the individual will be asked to complete the higher level vetting forms in the same way as current staff.

5.4 Should the individual already be engaged in the role while the vetting is taking place, it is the responsibility of the line manager to ensure that they are not carrying out any duties of that role where the higher level of vetting and screening is appropriate.

5.5 Should there be a requirement for the post holder to fulfil the duties of the role which require the higher level of vetting and screening (for example, in an emergency situation) approval for this must be sought in writing from the Assistant Commissioner, Operational Resilience and Special Operations and the Assistant Director, People Services.

6 Developed vetting

6.1 Developed Vetting (DV) is is the most detailed and comprehensive form of security clearance in UK government. It is needed for posts that require individuals to have frequent and uncontrolled access to TOP SECRET assets, or require any access to TOP SECRET codeword material.

6.2 The DV process includes a check of identity documents, employment and education references and has a minimum 10 years residency requirement .

6.3 Combined with the criminal records and credit reference checks, there are checks against security service records. Some references will be double checked and verified either by writing to or interviewing the individuals who provided them. The individual being vetted will also be interviewed by a Vetting Officer.

7 Maintaining and updating security and the appropriate level of vetting

7.1 For specific roles it may be appropriate to conduct regular security appraisals, to update or alter the level of clearance. The frequency of these updates may vary, up to and including an annual review, particularly if there is a significant increase in staff members access to sensitive information, systems or sites.

7.2 As a fail safe, Heads of Service should review vetting clearances for the staff in their departments on an annual basis. This will be to establish the checks already undertaken by HR Services and further measures required to protect personnel against potential vulnerability; access controls and safeguard information.

7.3 When a member of staff is resigning, retiring, or for any reason ceases to be an employee of the Brigade, it is staff's responsibility to return passes and appropriate equipment. Line manager's should ensure the brigade retrieve all appropriate equipment, passes, cards, and wallets. When the staff member provides notice of the end of employment, an LS1checklist is sent to the line manager detailing items to be returned. This may not cover every special item used, so if there is anything beyond the list like laptops, or wallets, they should be recovered too.

8 Outcome of vetting and screening

8.1 All results will be recorded on the Vetting Team system.

8.2 The Vetting Team will then notify the individual, the line manager and security adviser of the outcome.

8.3 The Vetting Team system automatically generates a renewal date which will be monitored and advised by the Vetting Team.

8.4 The Brigade reserves the right to ensure that an individual does not fulfil the duties requiring a higher level of vetting, withdraw an employment offer, or terminate employment, should the result be deemed unsatisfactory by the Brigade.

9 Observing security

9.1 It is incumbent on line managers to limit access to the Brigade or other organisation's assets, according to the requirements of the employees' role. In this way, staff are only given access to the information or systems they require to do their jobs.

9.2 Access to sensitive locations, assets or information should be limited to those for whom there is a genuine need for it. In exceptional circumstances physical controls may be used to restrict access to particularly sensitive areas.

It is important to record the issuing of passes, to monitor and review their use and to retrieve passes from staff when they cease employment or no longer require access to a particular location.

9.3 If the line manager of an employee leaving the Brigade is concerned any items may not be returned, they must notify People Services and TSS helpdesk asking for permissions attached to any Brigade swipe-card to be removed until informed by themselves, or anyone else within the immediate management chain.

10 Help and support

10.1 Please contact the Vetting Team in Operational Resilience..

Document history

Assessments

An equality, sustainability or health, safety and welfare impact assessment and/or a risk assessment was last completed on:

EIA	29/08/18	SDIA	H - 09/06/23	HSWIA	09/06/23	RA	

Audit trail

Listed below is a brief audit trail, detailing amendments made to this policy/procedure.

Page/para nos.	Brief description of change	Date
Throughout	Changes from People Services department creation.	28/03/2018
Throughout Page 4, para 7	This policy has been reviewed as current with amendments to department and team names to reflect the abolition of the London Fire and Emergency Planning Authority, now replaced with the London Fire Commissioner. New paragraph 'Developed Vetting' added. Please re-read content to familiarise yourself.	27/09/2018
Throughout	Policy reviewed as current.	24/07/2023
Page 2, para 1 Page 5, para 10	Introduction and policy statement consolidated. Help and support details added.	17/11/2023
Throughout	HR Services replaced with Vetting Team within Operational Resilience.	18/03/2024
Page 1	Departmental change of ownership from People Services as agreed with Assistant Commissioner.	22/03/2024

Subject list

You can find this policy under the following subjects.

Freedom of Information Act exemptions

This policy/procedure has been securely marked due to:

Considered by: (responsible work team)	**FOIA exemption**	**Security marking classification**