Personnel Security and National Security Vetting Policy

Version number: 1.0

Status: Published

Department/Team: People Services

Relevant policies: Recruitment and Selection Policy, Restructuring and Redeployment Guidance

Distribution: Internal

Author/Owner: People Services

Consultees: People Services, Vetting Sub-Group, trade unions, REACH Network, Pride Network, Access and Inclusion Network

Approved by: Sam McVaigh, Director of People Services

Application date: 17 December 2025

Review date: 17 December 2028

Security classification: Official

Key messages

This policy sets out the Information Commissioner's Office's (ICO) approach to personnel security and National Security Vetting (NSV). Its purpose is to:

- protect the ICO's assets, information and reputation by ensuring only trusted individuals who are entitled to work are employed or engaged;
- fulfil the ICO's legal and regulatory obligations under HMG Security Policy Framework (SPF) and Cabinet Office Guidance; and
- provide clarity on vetting requirements and processes.

Does this policy relate to me?

This policy applies to ICO employees, secondees, non-executive directors (NEDs), agency workers and third parties who require access to ICO data or systems. It is particularly relevant to roles where NSV clearance is required for the delivery of the ICO's statutory functions.

Table of Contents

Introduction

1.1. The ICO carries out standard personnel security checks in line with the government's Baseline Personnel Security Standard (BPSS) before individuals take up roles with us.

1.2. BPSS checks confirm the identity of individuals and provide assurance that individuals are suitable, trustworthy and legally able to begin work with the ICO.

1.3. The ICO handles sensitive information and may work with material classified for national security purposes. To manage this responsibly, some roles require NSV in addition to BPSS.

1.4. This policy explains how security checks and vetting apply from recruitment through to employment or engagement, and when someone leaves. It also sets out the responsibilities of

individuals and people managers in keeping clearances valid and reporting any changes that might affect them.

1.5. The rules in this policy follow government security standards, including the HMG SPF and guidance from UK Security Vetting. Holding the appropriate level of clearance is a condition of working in roles where NSV applies.

Back to the top

2. Baseline Personnel Security Standard

2.1. BPSS is a mandatory pre-engagement check and is conducted once a provisional offer of employment or engagement is accepted. BPSS is the minimum measure for anyone working for or in connection with any government department. It also underpins NSV.

2.2. In most cases, BPSS must be fully completed and passed before the individual starts work. This ensures compliance with government security standards and safeguards the ICO's operations, information and reputation. It also helps manage risks such as identity fraud, illegal working and falsifying employment history.

2.3. BPSS requires verification of four elements:

- Identity
- Employment history (past three years)
- Right to work in the UK
- Criminal record (unspent convictions only)

Further information on BPSS is available from the Cabinet Office.

2.4. People Services are responsible for completing BPSS for new employees before a formal offer of employment is made. For secondees, BPSS will be completed by People Services before their start date. For NEDs, the Department for Science Innovation & Technology (DSIT) complete BPSS and confirm to People Services once the check is complete.

2.5. Agency workers and contractors will not be engaged prior to completing BPSS. This must be included in the supplier contract. While there is an obligation on all suppliers working on public sector contracts to vet staff, which is reflected in supplier contracts, the ICO will validate the processes during the onboarding of suppliers for new contracts in the following high-risk categories:

- where supplier staff are working unsupervised on ICO premises; or
- where supplier staff require access to ICO networks, either through remote access or the provision of ICO laptops.

Some contracts, such as where supplier staff are handling sensitive physical data, may require enhanced vetting, which will be managed as required.

2.6. While Cabinet Office guidance allows for onboarding individuals who have previously passed BPSS, subject to additional checks in post, the ICO does not ordinarily adopt this approach. As the ICO is not part of the Civil Service Transfer Scheme, we are unable to formally verify previous BPSS clearance.

2.7. Where it is not possible to complete all elements of the BPSS in full, or where any check returns adverse information, People Services will conduct a risk-based assessment in consultation with the recruiting manager to determine the individual's suitability for employment or engagement.

2.8. The assessment will consider the nature and significance of the missing or adverse information, the requirements of the role, and any relevant mitigating factors.

2.9. The Director of People Services, as the designated risk-owner, will make the final decision either to:

- not employ the individual;
- employ the individual on a risk-managed basis; or

- following employment or engagement on a risk-managed basis, terminate the individual's employment if the acceptable risk level is exceeded.

Exceeding the acceptable risk level refers to any situation where the level of risk goes beyond what the organisation can safely tolerate. This may occur, for example, if new information comes to light, the individual's behaviour changes, or if they fail to comply with the risk management measures in place.

2.10. If an individual declines to undertake BPSS, their provisional offer of employment will be withdrawn. For NEDs and secondees, engagement will similarly not proceed if BPSS checks are declined.

2.11. For more information, on how personal information will be used for BPSS, please see the ICO's Privacy Notice.

Back to the top

3. National Security Vetting

3.1. NSV consists of additional security checks undertaken in addition to BPSS. These checks apply to individuals who will access sensitive information or assets, where compromise could cause significant damage to UK national security. These additional checks give greater assurance that an individual is suitable to have access to sensitive assets and information.

3.2. There are six levels of NSV:

- Accreditation Check (AC)/ Level 1A (1A)
- Counter Terrorist Check (CTC)
- Security Check (SC)
- Enhanced Security Check (eSC)
- Developed Vetting (DV)
- Enhanced Developed Vetting (eDV)

3.3. Depending on the level of NSV required, individuals may be asked to provide information about themselves and people closely connected to them.

3.4. Checks may also take account of financial circumstances (including credit and financial history, third party references or medical considerations) which could give rise to security concerns.

3.5. People Services submit applications for NSV. NSV clearance is issued by the Protective Security Centre (PSC), which processes applications and makes decisions.

3.6. Individuals undergoing NSV may request reasonable adjustments from the PSC as part of the vetting process, in line with the information and instructions provided to them.

3.7. The cost for all new clearances and renewals is charged to the recruitment budget held by People Services.

3.8. Where a role requires NSV, the required level of clearance will ordinarily be identified at the recruitment stage. This requirement will be clearly stated in the recruitment advert and job description as a condition of employment. Recruiting managers will decide whether NSV needs to be completed prior to commencement in the role. Applicants will not be expected to hold existing NSV.

3.9. Applications will only be initiated once right to work and identity checks have been successfully completed. Employment history and criminal record checks can be conducted after NSV applications are initiated, but must be completed before the NSV process is also complete.

3.10. Where it is decided that NSV can conclude after employment has commenced, it will be clearly communicated that there is a risk that clearance may not be achieved and that an individual's continued employment may be affected.

3.11. NSV may be carried out at any subsequent point after the commencement of employment when, for example, changes in

duties or responsibilities require it. Individuals will be advised by their people manager if and when they need to be subject to NSV.

Back to the top

4. Deciding on NSV levels for posts

4.1. Directors must regularly review the number and level of NSV clearances within their business area to ensure there are enough appropriately cleared individuals to deliver work that requires NSV. Where gaps are identified, Directors must plan for and request additional clearances in good time.

4.2. The Executive Director for Strategy, Resources and Transformation will have strategic oversight of the ICO's security clearance arrangements. This includes monitoring clearance levels across the organisation to ensure the ICO has the resilience needed to deliver current and future work requiring NSV.

4.3. In accordance with Cabinet Office guidance, NSV should only be applied where it is necessary, proportionate and adds real value, while ensuring that the ICO retains sufficient resilience in key areas requiring clearance for the delivery of statutory functions.

4.4. It is important to ensure individuals are cleared to a level appropriate to the degree of access to classified information they will have. When assessing a post for clearance, managers should be mindful that the clearance process is time consuming, costly and potentially intrusive. Costs and intrusiveness increase as clearance levels increase; therefore, managers must ensure clearance levels are proportionate to the role requirements.

4.5. For some roles that regulate or handle complaints about public bodies' or require engagement with information classified up to Secret or above, SC level clearance may be necessary.

4.6. NSV may also be required to support delivery of the ICO's wider statutory functions. When new roles are created, consideration should be given during implementation to whether any such roles require NSV clearance.

4.7. Some teams may, on occasion, require access to information classified at Secret or above, as part of the ICO's regulatory work with public bodies. Ensuring that these roles are identified and recruited to is the responsibility of local business areas. Depending on the nature of the work, DV or higher-level clearance may be required.

4.8. Guidance on clearance levels, including who needs each level and what each provides access to is available from UK Security Vetting.

Back to the top

5. When NSV cannot be obtained

5.1. Where a role requires NSV and an individual is unable to obtain the required clearance, or cannot do so within the necessary timeframe, there may be a risk to their commencement or continuation of employment or engagement.

5.2. For individuals who have not yet joined the ICO, offers of employment or engagement that are subject to NSV should be treated as conditional. If the clearance is refused, withdrawn, or not achieved within the required timescale, the conditional offer may be withdrawn.

5.3. For existing employees, this outcome is not automatic. Each case will be considered individually, taking into account all relevant circumstances. Where possible, adjustments to the role will be explored, and redeployment opportunities will be considered in line with the Restructuring and Redeployment Guidance. Termination of employment will only be considered as a last resort, where no suitable alternatives can be identified.

Any resulting employment decisions will be managed in accordance with the ICO's relevant policies and procedures. Employees have the right to appeal dismissal decisions and to raise concerns about redeployment through the Dispute Resolution Procedure.

5.4. Where applications are rejected because residency requirements for the level of clearance cannot be met, People Services will notify the individual and manager to review options for resubmission with supporting information.

5.5. The final decision regarding commencement or continuation of employment or engagement will rest with the Director of People Services, supported by advice from People Services and relevant stakeholders.

5.6. Individuals who are already working for the ICO and whose NSV clearance is refused or withdrawn may appeal the decision directly to the PSC, who will review the appeal and communicate the outcome to the individual. If the individual remains dissatisfied after the PSC's review, they may have a further right of appeal to the independent Security Vetting Appeals Panel.

5.7. Individuals who have not yet started work with the ICO at the time a vetting decision is made do not have a right of appeal.

Back to the top

6. Transferring NSV clearance

6.1. This section only applies to individuals joining the ICO from another organisation. NSV clearance is always linked to a sponsoring organisation. Holding a clearance with a previous employer does not guarantee it can be transferred to the ICO.

6.2. Whether a transfer can be accepted depends on factors such as the level of clearance, how recently it was granted or reviewed, and any changes in role requirements. Further conditions are set out in UKSV guidance, which People Services will consider when assessing transfer eligibility.

6.3. Individuals moving between roles within the ICO do not require a clearance transfer. However, a change of role may affect the level or type of clearance required, and this will be assessed as part of the recruitment or internal move process.

6.4. Where an individual who already holds NSV clearance is recruited to the ICO and has been identified as requiring NSV clearance for their job role, People Services will:

- submit a Transfer Request Form via the NSVS portal; or
- submit a new vetting application if the clearance cannot be transferred under UKSV rules.

6.5. Individuals must not assume they can access classified information or systems until the clearance transfer has been confirmed by People Services.

6.6. In cases where a transfer cannot be completed, a new application must be made, and continuation of employment or engagement may depend on the outcome.

Back to the top

7. Responsibilities for NSV maintenance and renewal

7.1. People Services are responsible for:

- Ensuring that any individual (including contractors or agency workers) who is put forward for NSV clearance has completed right to work and identification checks prior to the NSV application. Remaining BPSS checks will be completed in parallel.
- Maintaining records of all individuals' security clearances, including restrictions and renewal dates.
- Maintaining records of which roles require clearance and at what level.
- Co-ordinating applications for new, renewed or enhanced clearances.
- Notifying the PSC when individuals with NSV leave the ICO, are absent for more than 12 months, or no longer require the same level of clearance. To confirm, this does not require action from the individual.

7.2. Individuals who hold NSV clearance are responsible for:

- Knowing the date that they were granted clearance and understanding when it must be renewed.
- Initiating the renewal process at least three months before current SC clearance expires and six months before current DV clearance expires, where NSV remains a requirement for their role.
- Reporting immediately to their people manager or next most senior manager if an incident occurs or their circumstances change, that may affect their clearance in line with our disciplinary policy.
- Familiarising themselves with and following UK Security Vetting aftercare guidance. This includes reporting any changes in personal circumstances that could affect clearance, such as (but not limited to):
    - Identity and personal details
    - Residential circumstances
    - Financial circumstances
    - Criminal offences or police investigations.
    - Travel to certain countries or foreign contacts or interests that could affect clearance.
    - Other circumstances outlined in the UK Security Vetting aftercare guidance.
- Taking all reasonable steps to not access, attempt to access, or agree to view information for which they do not hold the appropriate clearance level.
- Completing the Security Appraisal Form (SAF) annually if holding DV clearance, ensuring all information is accurate and submitted on time. These forms are confidential assessments used to confirm that individuals continue to meet the standards required for access to sensitive

information, including ongoing eligibility, personal conduct and compliance with security responsibilities. For further information on SAF please see the UKSV Guidance.

In relation to travel to certain countries, individuals must notify the PSC as early as possible if they plan to travel or pass through any country identified as sensitive or high-risk. The PSC will provide advice on whether travel should be permitted, including any associated risks and appropriate mitigations, but does not give formal approval. After consulting the PSC, individuals must then contact People Services at the earliest opportunity for formal approval. People Services will advise on whether approval can be granted and signpost relevant internal policies on taking IT equipment abroad. For work-related travel, individuals must also comply with the Travel Overseas Guidance.

The list of sensitive or high-risk countries is available on the People Services Help app (Foreign Travel Notification Requirements for Security Clearance Holders). This list is updated as and when we are notified of changes.

Guidance and forms are available on the UK Security Vetting website (Aftercare and existing clearances - GOV.UK). Employees must follow these requirements as part of maintaining their clearance.

7.3. In addition to those individual responsibilities, people managers are responsible for:

- Supporting their direct reports undergoing NSV vetting, in collaboration with People Services. This may include directing them to UKSV guidance on completing applications, or referring them to wellbeing support.
- Ensuring in-year that their teams maintain the overall level of security clearance necessary to deliver ICO business needs.
- Managing restrictions to security clearances held within their team.

- Notifying People Services when an individual's role changes in a way that may affect the requirement for NSV clearance.
- Completing Aftercare Incident Reports (AIR) when required.
- Ensuring that SAFs are completed annually for individuals holding DV clearance.

7.4. Directors are responsible for:

- Regularly reviewing NSV requirements within their business area to ensure sufficient capacity for work requiring clearance.
- Confirming with the Executive Director for Strategy, Resources and Transformation that clearance levels are appropriate and sufficient across their teams.
- Supporting People Services in identifying roles that require NSV and ensuring recruitment plans reflect these needs.
- Ensuring that any changes in team structure or responsibilities that may affect NSV requirements are communicated to People Services.

Back to the top

8. Access to Secure Room and ROSA laptops

8.1. The ICO maintains a secure room for information relevant to its investigations and complaint handling work classified at the higher levels of security protection. The room also includes access to a secure BRENT fax/phone, as well as a secure document shredder.

8.2. Access to the secure room is restricted to authorised personnel only. Individuals must comply with ICO security procedures when entering or using secure rooms. Where an employee has responsibility for secure room access, this responsibility must be formally handed over if they leave the ICO.

8.3. In addition to the Secure Room, the ICO also has access to ROSA laptops for viewing information up to SECRET level. These

laptops can be used by individuals cleared to SC level and above who have undergone the mandatory ROSA training. This training must be refreshed annually.

8.4. Guidance on access, usage, handling of sensitive information, and protocols for leavers for both secure rooms and ROSA laptops is available in the Facilities and Estates Hub on Iris.

Back to the top

Feedback on this document

If you have any feedback on this document, please use this form to provide it.

Back to the top

Version history

Version	Changes Made	Date	Made by
1.0	Creation of new policy.	December 2025	People Services

Back to the top