HM Government

Change of Personal Circumstances Questionnaire: Criminal Conviction/Arrest/Caution

Important: Please read the notes on Page 3 and the Privacy Notice on Page 6 before completing the form

Please read the following instructions carefully.

You should complete this form if you hold a Developed Vetting (DV), Security Check (SC), Level 1B or Counter Terrorist Check (CTC) security clearance and you:

- Are arrested
- Are refused bail
- Receive a Police caution, reprimand or final warning
- Are convicted of an offence (other than minor road traffic offences)

1. Level of Clearance Held:

DV ☐ SC ☐ CTC ☐ Level 1B ☐

2. Your Details:

a. Surname/Family Name (now): **b. Title (Mr/Mrs/Ms/Miss/Dr/Prof/Rev):**

c. Gender:

d: Has your surname/family name changed since your current clearance was issued? Yes ☐ No ☐

If 'yes':
Please give your surname/family name at the time when your current clearance was issued:

Reason for surname/family name change:

e. Full Forenames:

f. Have your forenames changed since your current clearance was issued? Yes ☐ No ☐

If 'yes':
Please give your forenames at the time when your current clearance was issued:

Reason for change of forenames:

g. Date of Birth: Day ☐ Month ☐ Year ☐

h. National Insurance Number:

i. Town of birth:

County/region of birth:

Country of birth:

j. Current grade/rank/position (if applicable):

k. Job Title (if applicable):

l. Staff or Service Number (if applicable):

3. Your Contact Details

a. If we need to contact you, do you want to be contacted at: Home ☐ Work ☐ ?
(We will try to meet your preference but this cannot always be guaranteed)

b. Please enter your home address:

Flat Number: House Number: House Name:

Street:

District:

Town:

County/Region: Postcode:

Country:

c. Please enter your work address:

Name of Employer:

Building Number: Building Name:

Street:

District:

Town:

County/Region: Postcode:

Country:

d. Contact telephone numbers (in order of preference). If you are not providing a contact e-mail address, you must enter at least TWO separate telephone numbers.

Preferred contact number:

Alternative contact number:

Alternative contact number:

e. Contact e-mail address:

STATEMENT OF HMG PERSONNEL SECURITY AND NATIONAL SECURITY VETTING POLICY

Minimum Personnel Security Controls

1. It is HM Government's policy that all areas of government and the national infrastructure should include in their recruitment processes certain basic checks. These checks include verification of the applicant's identity, employment history, their right to work in the UK and, if appropriate, checks of any unspent criminal records. Within government these controls are described in the Baseline Personnel Security Standard. In addition, the Centre for the Protection of National Infrastructure (CPNI) produces a range of relevant guidance on personnel security and makes similar advice available to the wider national infrastructure.

National Security Vetting

2. National security vetting comprises a range of additional checks and may be applied where a risk assessment indicates it is proportionate to do so. The risk assessment process takes account of the access an individual may have to sensitive assets (physical, personnel or information) at risk from a wide range of threats. These threats include: terrorism, espionage, or other actions that could threaten the United Kingdom. The requirements of international agreements concerning the protection of allies' information may also inform such assessments.

3. It is government policy that individuals should not be expected to hold an existing security clearance in order to apply for posts that require vetting, except where such posts are short term and need to be filled urgently.

4. There are a number of types of national security vetting clearance. Before any such clearance is undertaken the requirements of the Baseline Personnel Security Standard must be met. Whilst the information required and the range and depth of checks undertaken at each level may vary, they are all intended to allow Government departments and agencies, the Armed Forces and police forces to assess whether individuals who are to be employed in sensitive posts or critical functions might represent a security risk either directly or indirectly.

Checks

5. Individuals subject to national security vetting (including UK nationals taking up sensitive posts in international organisations) will be asked to provide via questionnaire personal information about themselves, partners, family members and other associates. It may be checked, and retained for future checks, against:

- **Relevant personnel records held by the employing department or company**
- **Criminal records (both spent and unspent as defined by the Rehabilitation of Offenders Act 1974)**
- **Information held by the Security Service.**
- **Credit reference agency records**

6. The process may also take account of:

- **Financial circumstances generally**
- **Third party character references**
- **Any medical considerations that could give rise to security concerns**

7. Interviews with the vetting subject and referees may be carried out to establish good character and to verify information that has been provided.

Decision Making

8. National security vetting decisions may only be taken by Government departments, agencies, the Armed Forces or police forces. All the available information is taken into account to reach a reasoned decision on an individual's suitability to hold a security clearance.

9. Security clearances may be refused or withdrawn where:

- **There are security concerns related to an individual's involvement or connection with activities, organisations or individuals associated with the threats described in this Statement (or any similar new threats that emerge);**
- **Personal circumstances, current or past conduct indicate that an individual may be susceptible to pressure or improper influence;**
- **Instances of dishonesty or lack of integrity cast doubt upon an individual's reliability;**
- **Other behaviours or circumstances indicate unreliability.**

10. Wherever possible existing employees will have an opportunity to discuss, comment on and challenge any adverse information that arises. However in certain circumstances it may not be possible to share such information as this could compromise national security, the public interest or third party confidentiality.

Avenues of Appeal

11. Existing employees who are subject to national security vetting and either refused a security clearance or whose clearance is withdrawn may appeal against such decisions. All departments and agencies that carry out national security vetting must provide for an internal appeal process. Where individuals remain dissatisfied they may appeal to the Security Vetting Appeals Panel, an independent body.

12. The Panel will consider the case, review the information and invite the appellant and the organisation to make representations. The Panel will make recommendations to the Head of Department or organisation in the light of its findings as to whether the decision should stand or be reviewed. The Panel may also comment on the security vetting procedures and adequacy of the internal appeal arrangements.

13. There are no national security vetting appeal routes for applicants for employment who are refused a security clearance. Separate arrangements exist for applicants, employees and contractors of the security and intelligence agencies, who may complain to the Investigatory Powers Tribunal. Any individual may apply to an Employment Tribunal if they feel that they have been discriminated against in any part of the recruitment process.

Ongoing Personnel Security Management

14. The national security vetting process provides an assessment of the vetting subject at the time the process is carried out but active ongoing personnel security management is required to ensure that a security clearance maintains its currency. As a minimum this will involve active consideration of the vetting subject's continuing conduct in respect of security matters; it will also require checks to be repeated at regular intervals.

Please note that any information provided will be treated in strict confidence. In cases where a potential risk is identified, and a decision taken to 'manage the situation' rather than refuse security clearance, those tasked with managing that risk will need the appropriate information in order to do this effectively.

Failure to disclose relevant circumstances or information is likely in itself to be regarded as evidence of unreliability and will be taken into account when assessing your suitability for security clearance. It is therefore in your own interests to be honest and open in the information you provide in this questionnaire.

4. Details of the Incident

a. I am reporting a: Conviction ☐ Arrest ☐ Caution ☐ Other ☐

b. Please give full details:

c. Please give the date on which this occurred Day ☐ Month ☐ Year ☐

Declaration

I declare that I have read and understood the statement of HM Government's policy on vetting on page 3 of this questionnaire.

I understand that in accordance with this policy the personal information that I have provided on this form about myself, my partner
(if applicable) and my family will be submitted for checking against national criminal and security records

I understand that a check against credit reference agency records and investigations into my financial circumstances will also be carried out. I understand, too, that the information provided may be subject to ongoing checks where they are necessary and proportionate.

I declare that the information I have given is true and complete to the best of my knowledge and belief, and I understand that any false statement or deliberate omission in the information I have given in this questionnaire may disqualify me from employment (including employment in connection with Crown contracts if applicable) or make me liable to disciplinary action, which may include dismissal.

I undertake to notify any material changes in the information I have given above (e.g. change of partner, address or financial circumstances), including any future criminal convictions, to the Personnel or Security branch concerned.

Important: Data Protection legislation. This questionnaire asks you to supply "personal" and "sensitive personal"data as defined by current Data Protection Act legislation. You will be supplying this data to the appropriate vetting authority where it will be processed exclusively for the purpose of security vetting, , in accordance with HM Government's vetting policy, save that, in the highly unlikely event that data supplied by you discloses or suggests that:

i. a criminal offence has occurred or is likely to occur or,

ii. staff may be at risk of danger e.g. if you have been diagnosed with a serious mental condition as potentially endangering yourself or others

then the vetting authority may pass on that information alone to the appropriate person(s). Subject to this, the vetting authority will protect the information which you provide and will ensure that it is not passed to anyone who is not authorised to see it.

By signing the declaration on this page, you are agreeing that you understand that the data you provide in this questionnaire will be processed in the manner described above.

If you have any concerns about any of the questions we ask, or what we will do with the information you provide, which are not answered by the guidance notes please contact the person who issued this form for further information.
Note: Please review the form BEFORE SIGNING to ensure that all questions have been fully answered.

Signed: | **Date:** Day | Month | Year

Privacy notice for processing personal data throughout National Security Vetting (NSV)

This privacy notice applies when the vetting provider is United Kingdom Security Vetting (UKSV). UKSV is part of the Cabinet Office. If you are unsure as to the identity of your vetting provider, please ask your sponsor, which is normally your employer. This notice explains how we intend to store and handle your personal data and that of third parties in the course of conducting NSV. This notice may be updated from time to time – the latest version will be available on gov.uk.

This notice applies in relation to all previous and current NSV applications processed by UKSV or its predecessors (Defence Business Services and FCO Services) and should be read in conjunction with the NSV forms and Her Majesty's Government's (HMG's) Personnel Security Controls policy.

1. The identity of the NSV data controllers

1.1. UKSV is responsible for carrying out NSV and, for some of its customers, also makes the clearance decision. In these circumstances, together with the Security Service, UKSV is a data controller for the NSV process. As UKSV is part of the Cabinet Office, the Data Protection Officer ("DPO") responsible for NSV can be contacted via the details in paragraph 11.4.

1.2. When UKSV carries out NSV, but the decision on whether to grant security clearance is taken by the sponsor (which is normally the public authority employer), the sponsor organisation is a joint data controller with UKSV. In these circumstances, if you wish to exercise your rights under data protection legislation, you can contact either UKSV or the sponsor organisation that decides whether you will be granted security clearance. It is the sponsor's responsibility to advise you of their contact details.

1.3. In addition to UKSV and the sponsor organisation, the Security Service is a data controller for NSV in respect of the check of Security Service records. The Security Service publishes advice on access to information here. It can be contacted via:

- The Enquiries Desk,
- PO Box 3255,
- London, SW1P 1AE.

1.4. Should you be granted clearance and subsequently move to another post requiring NSV at a different organisation, the relevant personnel security risk owner for the new organisation may review your clearance against the particular security risks that organisation faces. In such circumstances, the new organisation replaces the initial sponsor organisation as a joint data controller for NSV.

2. Why we will process your data

2.1. We will process your personal data for the purpose of carrying out NSV, including aftercare. We will also process the data of third parties where explicitly required in order to conduct your case. NSV is necessary and proportionate to safeguard the UK's national security. We may also process your data for ancillary purposes, for example, to facilitate an appeal to the Security Vetting Appeals Panel, to fulfil legal and regulatory requirements, for research for ongoing monitoring, or in an anonymised manner for business monitoring and planning purposes.

3. The legal basis for the processing

3.1. UKSV and the sponsor organisation process your personal data and that of third parties in accordance with the General Data Protection Regulation, as applied by Chapter 3 of Part 2 of the Data Protection Act 2018 ('the Applied GDPR'). The Security Service will process your personal data in accordance with Part 4 of the Data Protection Act 2018 (intelligence services processing).

3.2. The processing of your personal data and that of third parties is necessary for the purpose of NSV. The legal basis for the processing of data as part of NSV is that it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller (Article 6(1)(e) Applied GDPR). Where vetting providers process special category data their lawful basis for doing so is that processing is necessary for reasons of substantial public interest for the exercise of a function of the Crown, a Minister of the Crown, a government department, or the exercise of a function conferred on a person by an enactment (paragraph 6, Schedule 1, Data Protection Act 2018). Conducting NSV is a function of UKSV, which is part of the Cabinet Office, a government department.

4. How your data will be processed

4.1. Your personal data and that of third parties will be processed as described in 'HMG Personnel Security Controls', currently as per **Annex A** 'Statement of HM Government Personnel Security and National Security Vetting Policy', on page 17. The categories of personal data which we process are described in those documents.

5. Who we share your data with

5.1. Personal data that we collect and process for NSV is very strictly controlled and protected by a robust level of physical, cyber and personnel security measures. Your NSV personal data is kept separate from other personal data and access is only provided to those with a strict need to know for the purpose of conducting your NSV, such as your vetting officer.

5.2. ***Conducting NSV -*** To conduct the various checks that form part of NSV, it will be necessary to share some of your personal data with the relevant check provider so that they may provide further personal data to us. We only share the minimum amount of data necessary to enable the provider to perform the check. In most cases this is limited to basic identifying information (such as your name or date of birth) to ensure that the provider is checking the correct individual. In exceptional circumstances it may contain additional data fields to disambiguate between you and another individual, for example if you share their name and date of birth.

5.3. To perform the component NSV checks and reach a security clearance decision, UKSV may share some of your data with:

- Your employing organisation (e.g. to request access to relevant personnel records)
- Public authorities which maintain criminal records databases.
- The Security Service.
- Credit reference agencies.
- Character referees (e.g. a past academic supervisor).
- The sponsor or personnel security risk owner (e.g. to enable them to make a decision on your suitability to hold security clearance or so that they can specify any risk mitigation measures conditional for your clearance).

5.4. Third party personal data may be processed as a result of these checks. For example, a character referee for your case would need to share some basic personal data with the UKSV vetting officer.

5.5. Data provided to credit reference agencies as part of NSV checks may be used to update that agency's record of an individual (e.g. a new surname), the updated version of which will subsequently be employed throughout that agency's routine business activities. Currently, UKSV employs the services of Experian as part of NSV checks, but it may be necessary to appoint an alternative or additional credit reference agency in future, in which case this notice will be updated. It is important that you read and understand Experian's Privacy Policy in conjunction with this NSV Privacy Notice. We may request that you confirm that you have done so, and we will retain that confirmation for our records.

5.6. ***Awarding or removing clearance*** - Following your application, your sponsor and employer will be notified whether your clearance has been granted or refused. Your sponsor and employer will also be notified in the event that an existing clearance has withdrawn or been revoked.

5.7. ***Risk mitigation -*** On rare occasions where a security risk has been identified, UKSV or the sponsor department may consider that it is possible to mitigate that risk to an acceptable level by sharing relevant information with an appropriate person within your line management chain. Should this apply to you, we will not share your personal data without discussing this with you first and obtaining your explicit agreement. If we seek to do this we will give you further explanation of the reasons why and purpose, and also explain your rights with regard to providing and withdrawing agreement. Note that you withholding agreement may render risk mitigation impossible, and therefore lead to a refusal to grant clearance. If you are worried about the confidentiality of the NSV process, please contact your sponsor for advice.

5.8. ***Public interest matters -*** Very exceptionally, data supplied by you or by a third party may be sufficiently serious that the NSV data controllers may consider it is necessary and in the public interest to share relevant information with an appropriate authority, such as the police. This might occur when information suggests that:

- you may have committed a previously undetected criminal offence, or that an offence may be about to be committed;
- you or others may be at risk of harm; or
- action is required to safeguard national security.

5.9. ***Appeal*** - If your clearance is refused or withdrawn and you decide to exercise a right to appeal, we will need to provide the relevant authority considering your appeal with relevant personal data to enable them to do so.

6. How long we will keep your personal data

6.1. Your personal data and that of third parties will be retained for so long as is necessary for the purpose for which it was collected (i.e. safeguarding national security). Personal data collected during the NSV process will be retained by UKSV and the sponsor organisation for fifteen years from the date that your security clearance expires, or is withdrawn or revoked. However, in exceptional circumstances it may be necessary to retain personal data beyond this period, such as in the interests of national security or to defend legal proceedings which have already commenced.

7. Your data rights

7.1. You have considerable say over what happens to your personal data. Your rights and how you may exercise them are fully detailed on the independent Information Commissioner's Office

website. In relation to your personal data held by UKSV or the sponsor organisation, unless an exemption applies, you have the right to:

- request a copy of your personal data;
- require us to restrict the processing of your data in certain circumstances;
- request your data be deleted or corrected;
- object to the processing of your data; and
- to lodge a complaint with the independent Information Commissioner's Office (ICO) if you think we are not handling your data in accordance with the law. Their contact details are provided in paragraph 11.3.

8. International data transfers and international organisations

8.1. As described above, for important reasons of public interest and national security (Article 49(1)(d) Applied GDPR), it may be necessary for UKSV to seek information from referees, some of whom may be from international organisations, EU member states, or located in countries where the EU Commission has not issued an adequacy decision to confirm that it considers the country provides an adequate level of data protection. This paragraph will be kept under review subject to the outcome of ongoing UK-EU negotiations, and subsequent arrangements at the end of the UK-EU transition period.

8.2. Where the sponsor organisation is an international organisation, for example NATO, or where your clearance is to work for a contractor overseas, we will inform the organisation or contractor whether your clearance is granted or refused, or has been withdrawn or revoked. In the event that there is an information sharing agreement with the party in question, this will be communicated to you as part of your clearance process.

9. Decisions based on automated processing

9.1. NSV decisions are never based solely on automated processing. The decision whether to grant or refuse security clearance is always taken by the relevant personnel security risk owner.

10. Failure to provide data

10.1. You are required to provide the personal data requested as part of NSV in order to obtain the requisite clearance for your role, which may be either a contractual requirement or mandatory for your employment with the relevant organisation. If you do not provide the requested data, we will be unable to grant you security clearance and this may impact on your employment.

11. Complaints

11.1. If you are not satisfied with the way in which your personal data is being processed by UKSV you can make a complaint to the Business Support Team:

- UKSV Business Support,
- Imphal Barracks,
- York, YO10 4AS.
- Email: UKSV-BusinessSupportRequests@mod.gov.uk.

11.2. The team will acknowledge your complaint within 5 working days and endeavour to send you a full response within 20 working days. If the team is unable to respond within these timeframes, they will explain why and let you know when you can expect a fuller response.

11.3. If you are not satisfied with the response, you have the right to lodge a complaint with ICO if you think we are not handling your data in accordance with the law. They can be reached via this link or by calling 0303 123 1113.

11.4. You can also contact the Cabinet Office Data Protection Officer, who provides independent advice and monitoring of Cabinet Office's use of personal information. They can be reached via:

- Data Protection Officer,
- Cabinet Office, 70 Whitehall, Room 405,
- London, SW1A 2AS.
- Email: dpo@cabinetoffice.gov.uk.