Cabinet Office

UK Government Baseline Personnel Security Standard

Policy and guidance on pre-employment checks for all individuals working for government.

Version 7.0 – June 2024

Contents

Foreword

This document forms part of the Government Functional Standard GovS 007: Security that promotes consistent and coherent ways of working across government. They can be found at GOV.UK.

Functional standards cross-refer to each other where needed, so they can be confidently used together.

Consistent language is used which contains mandatory and advisory elements and is defined in the table below. It is assumed that legal and regulatory requirements are always met.

Term	**Intention**
Shall	Denotes a requirement: a mandatory element.
Should	Denotes a recommendation: an advisory element
May	Denotes approval.
Might	Denotes a possibility.
Can	Denotes both capability and possibility
Is/Are	Denotes a description

Document Structure

This document outlines the requirements for the Baseline Personnel Security (BPSS) policy. Some chapters may have a **box** to denote a **policy principle** which is the high-level objective for a policy.

Purpose and Background

Introduction

1. The Baseline Personnel Security Standard (BPSS) ensures organisations are employing individuals who have the right to work, with the honesty and integrity required for working within and/or for the government.

2. This guidance is for government organisations or third parties (suppliers) conducting BPSS checks.

3. BPSS is a series of checks conducted once a provisional offer of employment is accepted by individuals. A formal offer **shall** only be made once BPSS is passed. BPSS **is not** a national security vetting (NSV) clearance. It applies to **all individuals** working within and for the government, such as civil servants, contractors, members of the armed forces, temporary staff and suppliers. The purpose is to:

    a. Ensure that all individuals are entitled to take up employment;

    b. Protect the security of the government estate and its assets; and

    c. Provide a basis for NSV, if a security clearance is required.

4. BPSS comprises **four main checks** for an individual. Guidance is provided within the relevant sections in this document:

    a. Identity (ID);

    b. Right to work (RTW) in the UK;

    c. Employment history; and

    d. Criminal record (unspent convictions).

5. Organisations **can** apply security controls and checks in addition to paragraph 4 in line with the organisation's risk appetite. See **Additional Checks** for further information.

6. BPSS addresses potential risks such as identity fraud, illegal working and falsifying employment history. Failure to address these issues could lead to financial or reputational damage, and loss of sensitive information for the UK government.

7. BPSS **shall** not discriminate against individuals who might face barriers to employment. This might include for example, individuals with neurodiversity or from a lower socio-economic background. Further information can be found via Going Forward into Employment (GFiE). Organisations **shall** assess each individual on a case-by-case basis.

8. If the BPSS cannot be completed, or the checks identify an adverse concern, the organisation **shall** either:

a. Risk-manage and onboard the individual, for example this may occur when the individual has limited UK residency. Guidance is provided within the relevant sections of this document.

b. Not employ the individual, for example if they do not pass RTW checks.

Access entitlements

Policy Principle: BPSS **shall** give individuals access to information only required for their role.

9. BPSS enables access to government information which **shall** be securely managed. The Government Security Classification Policy (GSCP) outlines the proportionate security controls and baseline behaviours to be followed across government.

10. Organisations **shall** provide individuals who have passed BPSS access to UK OFFICIAL information and assets. Where required, under applicable international agreements/arrangements, BPSS **can** provide access to international RESTRICTED classified information. Further information on protecting and exchanging international classified information is on GOV.UK.

11. Organisations **may** provide exceptional supervised access to UK SECRET information or assets (such as IT systems or sites), following written authorisation from their security teams. National Security Vetting is required for regular access.

12. BPSS **shall not** allow:

    a. Access to roles where the individual can obtain a comprehensive picture of a SECRET plan, policy or project.

    b. Access to, or knowledge of, assets belonging to another country or international CONFIDENTIAL classified information or above (for example NATO CONFIDENTIAL).

    c. An overseas supplier or contractor to have access to, or knowledge of, assets classified SECRET or above.

    d. Access to a restricted site during an overseas visit, which is a government, military or industrial facility cleared to hold classified material.

    e. Access to any SECRET codeword material or TOP SECRET material.

Roles and Responsibilities

13. The Government Security Group (GSG) in the Cabinet Office is responsible for the BPSS policy. This document **should** be read in conjunction with the Government Functional Standard GovS 007: Security.

14. Human Resources (HR) teams are generally responsible for administering BPSS and its information management. Organisations **may** conduct the BPSS within their security team.

15. HR, Security or other relevant teams **shall** work together to ensure BPSS is effective and consistently applied.

    a. Other stakeholders **should** also be involved where appropriate, for example: legal advisers, counter-fraud, commercial and procurement teams.

    b. Security teams **should** assess any adverse criminal check results or cases where satisfactory checks could not be conducted.

16. Organisations **shall** determine the roles and responsibilities with a supplier. This includes creating or updating contracts or signed agreements as necessary.

Outsourcing

Policy Principle: Organisations **shall** protect their information, even if it is managed by suppliers.

17. Organisations **may** outsource parts, or the entire BPSS process to a supplier. This includes the decision to grant BPSS.

18. Organisations **should** conduct a risk assessment on all procurement to ensure the security of their supply chain. Organisations accept the risk if this is not conducted. The organisation's Security Adviser (or equivalent) will be able to advise. The National Protective Security Authority (NPSA) has guidance on procurement.

National Security Vetting (if applicable)

Policy Principle: BPSS **shall** assess an individual's suitability for employment. NSV **shall** assess an individual's suitability to hold a security clearance.

19. For some roles, an individual may be required to undergo BPSS and obtain NSV. Organisations **shall** determine whether a national security clearance is required for a role, further guidance is in the HMG Personnel Security Policy.

20. Identity and RTW checks **shall** be completed prior to NSV applications being initiated.

21. Criminal record (unspent) and employment history checks **can** be conducted after NSV applications are initiated, however organisations **shall** complete them prior to NSV clearance being granted.

22. Organisations **shall** confirm to UKSV as part of the NSV initiating process whether partial or full BPSS checks have been completed. If an NSV application is initiated with

partial BPSS checks completed, as per paragraph 21, the decision maker must be assured full BPSS checks have been completed prior to granting NSV clearance.

Previous History of Fraud Against Government

23. The Public Sector Fraud Authority's (PSFA) Internal Fraud Hub receives the details from participating government organisations of civil servants who have been dismissed, or who would have been dismissed had they not resigned, for internal fraud. In instances such as this, civil servants are then banned for five years from further employment in the civil service, within participating organisations.

24. Participating government organisations **shall** carry out pre-employment checks on all appointments which fall within scope of the Internal Fraud Hub policy using the data on the Internal Fraud Hub to detect instances where known fraudsters are attempting to reapply for roles in the civil service. More information on the Internal Fraud Hub privacy notice and the Public Sector Fraud Authority can be found on GOV.UK.

Data protection in recruitment and selection

Policy Principle: Organisations **shall** protect personal data obtained during the BPSS process in accordance with legislative and regulatory requirements.

25. Organisations **shall** outline how personal information will be used for BPSS in their privacy notice. This includes any agreements with suppliers.

26. Organisations **shall** inform the individual that refusing to undertake BPSS **shall** lead to a withdrawal of an offer of employment.

27. For organisations using Civil Service Jobs, the data responsibilities are:

    a. Cabinet Office is the data controller for the individual's account details, user research materials, and for any job applications not submitted.

    b. Cabinet Office and the organisation the individual applies to are joint data controllers for the personal data within any submitted applications.

28. If organisations are using a supplier other than Civil Service Jobs, they **shall** determine their roles and responsibilities with their supplier.

Joiners and Movers

Introduction

29. BPSS checks apply to an individual's recruitment process, irrespective of their employment type. Organisations **shall** process personal information in accordance with their policies and processes.

BPSS Policy

30. When an individual accepts a provisional offer to join an organisation, irrespective of whether the individual has previously passed BPSS, that organisation **shall** complete the following before providing a formal offer to the individual:

    a. Identity and RTW checks to meet their legal obligations (guidance is provided within the relevant sections in this document).

    b. All BPSS checks for individuals who have not undergone it before.

31. In addition, organisations **can:**

    a. Conduct the criminal record (unspent) and employment verification checks in line with their risk threshold.

    b. Conduct alternative verification and assurance checks if verification cannot be conducted as outlined in this document. Please refer to paragraph 8.

32. Organisations **can,** if individuals have previously passed BPSS, onboard them and run relevant additional checks while they are in post in line with their risk threshold (see **Additional Checks** section). This might occur for example when high numbers of contractors are surged for government public services. Individuals **shall** only be onboarded after identity and RTW checks are completed, in conjunction with organisations' internal policies.

    a. Organisations **shall** make clear that continued employment is dependent on passing the relevant additional checks. They **should** be completed within three months of employment commencing. If an individual fails any element, their employment **may** be terminated.

Sifting and shortlisting

Policy Principle: BPSS is a pre-employment check and **shall not** be used to sift potential candidates.

33. Recruitment for the Civil Service **shall** be made on merit on the basis of fair and open competition in accordance with the Civil Service Recruitment Principles.

Identity Verification

Introduction

34. Verifying the identity of the candidate ensures a role is given to the correct person. This avoids employing someone who is using a fake ID, is pretending to be someone else, or does not have the right to work in the UK.

35. One or both of the following checks for identity verification **shall** be conducted.

    a. A physical check - conducted by the relevant team. Document verification guidance is available from the National Document Fraud Unit and NPSA.

    b. A digital service - the organisation uses an Identity Document Validation Technology (IDVT) provider.

36. If organisations use a digital service, they **should** make their own arrangements with a government approved service provider through their procurement channels. Organisations **shall** assure themselves of the results of any digital identity verification service used.

Identity Documentation

37. Organisations **shall**:

    a. Verify documentation which evidences the individual's full name, date of birth and full current and / or permanent address using one or more of the documents in **Annex A**.

    b. Verify a photograph ID of the individual. If individuals do not have photo ID, they **should** be asked to provide additional identifying documents from **Annex A**. Please also refer to paragraph 41.

    c. Obtain a copy of the original document, or IDVT identity check output, and securely store it in line with the organisation or the supplier's data retention periods.

38. If a physical check is used to verify identity, documentation **shall** be verified physically on or before an individual's first day of employment. Guidance is available from the Home Office Employer's Guide to Right to Work Checks, the Good Practice Guide (45) on GOV.UK and the National Document Fraud Unit.

39. If IDVT or share codes are used to verify identity, organisations **shall** verify the photograph and biographic details on the outputs are consistent with the individual presenting themselves for work.

40. Organisations **can** accept some official digital documents such as bank statements and utility bills as original documents - see Annex A Group B.

Countersignatory

41. If an individual is unable to provide suitable identifying documents (for example because of age, lack of residence or socioeconomic background), organisations **shall** make a risk based decision with what evidence the individual provides, following the Employers Guide to Right to Work Checks.

42. That risk based decision **can** include requesting a statement and signed passport photograph of the individual from a countersignatory. Any documentation received from a countersignatory **shall** be checked by the employing organisation or supplier.

    a. The countersignatory statement **shall** state:

        i. How long they have known the individual. This must be at least **two** years.

        ii. The full name and address of the individual

        iii. Work in (or be retired from) a recognised profession or be 'a person of good standing in their community'.

        iv. The countersignatory contact details. This **should** be their work address or work email, unless they are retired

    b. The signatory **should** be contacted to confirm their profession and that they completed the statement.

Right to Work Verification

Introduction

43. Organisations are legally required to check the individual has a right to work in the UK.

44. There are three types of verification checks for right to work:

    a. A physical check of an immigration document - conducted by the relevant team, see paragraph 38.

    b. A digital service - the organisation uses an IDVT provider, see paragraph 39.

    c. Online Home Office right to work check for non-British or non-Irish Citizens.

45. Organisations **shall** conduct a Employer Checking Service if an individual's nationality and immigration status cannot be verified, or concerns remain. This checks if an individual:

    a. Cannot show their documents or online immigration status.

    b. Has a digital or non-digital 'Certificate of Application' that states the Home Office must check their right to work.

    c. Has an Application Registration Card (Application Registration Cards must state that the work the employer is offering is permitted).

Civil Service Nationality Rules

46. Roles within the Civil Service have additional nationality requirements (including Reserved Posts) which is governed by the Civil Service Nationality Rules (CSNR). The CSNR applies to Civil Servants only, and does not apply to other employment groups. The CSNR outlines the eligibility for employment in the Civil Service on the grounds of nationality, and **shall** be followed by government departments and other bodies.

Overseas Residency Checks

47. A lack of UK residency **may not** be an automatic bar to employment. However, individuals may need to have resided in the UK for a sufficient period of time depending on the role's requirements.

48. If individuals have resided overseas for six months or more within the last three years, organisations **shall** assure themselves by requesting one or more of the following original documents below, this is not an exhaustive list:

    a. Proof of overseas residence.

    b. Overseas employee or academic references.

c. References from UK departments and agencies based overseas for example Foreign Commonwealth and Development Office (FCDO) missions, British Council, non-government departments organisations and agencies.

d. Where available, official and verifiable overseas police certificates obtained from the country or countries of residence, see **Criminal Record Check Verification (unspent convictions)** section.

49. Where appropriate, confirmation of dates **should** be obtained from passports and work permits by contact with appropriate Embassies, High Commissions and Consulates.

Employment History Verification

Introduction

50. Verifying an individual's employment history reduces the risk of fraud by corroborating their previous roles. It also allows the employer to review any significant gaps (such as unemployment, periods overseas), omissions or potential conflicts of interest.

51. Organisations **shall**:

    a. Verify an individual's disclosed **employment, academic history and/or qualifications (where applicable)**, for a minimum of three years prior to BPSS checks being conducted. This **can** be conducted via His Majesty's Revenue and Customs (HMRC) PAYE, or by employer references.

    b. Advise individuals that by providing contact information for references, they are providing consent for those referees to be contacted.

    c. Verify the individual's employment history if they are self-employed. This includes confirming the dates of the individual's self-employment and the status of their business. Acceptable documents or checks include evidence from HMRC, bankers, accountants, solicitors, trade or client references.

52. Organisations **should**:

    a. Obtain references or evidence if there are gaps of six months or more (continuous or cumulative) within the previous three years from the individual.

        i. However, organisations **can** check employment gaps above this requirement to meet their risk threshold.

53. Organisations **can** accept a HMRC PAYE records PDF from an individual as proof of employment.

Criminal Record Check Verification (unspent convictions)

Introduction

54. The Rehabilitation of Offenders Act 1974 enables employers to ask individuals for any unspent criminal convictions and applies in England, Wales and Scotland. The Act states that if an offender remains free of further convictions for a specified period (the "rehabilitation period") the conviction becomes "spent". Once spent an individual must be treated as if the offence had never been committed.

55. There are some **exceptions:** full disclosure of all convictions and cautions are required for jobs or activities relating to, among others, national security or law enforcement. The individual **shall** be informed if full disclosure is required. Further information is on GOV.UK.

56. Rehabilitation periods vary for Scotland and Northern Ireland. Organisations **should** consult with their legal or security teams if they have any questions.

Criminal Record Check (unspent)

57. Organisations **shall**:

    a. Conduct an unspent criminal records check with the relevant UK and Northern Ireland authorities: Disclosure and Barring Service (DBS, covering England and Wales), Disclosure Scotland and AccessNI - this will incur a fee. Organisations **shall** consider the differing rehabilitation periods between England, Scotland and Northern Ireland in their risk assessments.

        i. These organisations **might** not accept digital documents to conduct criminal record checks.

    b. Record the outcome of the disclosure on the individual.

    c. Discuss a criminal record result with the relevant teams and prepare a risk assessment. GOV.UK has guidance on recruiting someone with a criminal conviction. The risk assessment **should** provide the basis for any ongoing personnel security queries.

    d. Ensure staff carrying out the checks are completely satisfied with the information and documents that the individual has provided. If there are any concerns, they **should** speak with their HR or security team.

58. Organisations **should** offer individuals an opportunity to explain any disclosures or discrepancies and provide applicable supporting evidence as soon as possible.

59. Organisations **can** accept a Basic Disclosure Certificate. If it is older than 90 days from the date of issue, organisations **can** accept it in line with their risk appetite, however there is no official expiry date for a criminal record check issued by DBS. They are not

job specific and are generally issued to the individual, but can be provided directly to organisations with the individual's consent.

a. Organisations **should** consider that the DBS certificate is a snapshot in time for the individual.

b. Organisations **shall** ensure it matches the identity documents of the individual and retain a copy in line with their data retention policy.

60. If it is not possible to obtain a certificate from DBS, Disclosure Scotland or AccessNI because of a lack of UK residence, departments **shall** find alternative means of assurance in line with their risk appetite. See further guidance in **Overseas Criminal Record Checks**.

Considering Unspent Convictions

Policy Principle: A criminal conviction **should not** be an automatic barrier to employment and **shall** be assessed on a case by case basis.

61. If unspent criminal convictions have been disclosed, organisations **shall** consider the factors below. Assessments against these factors **should** be recorded and stored in line with the organisation's data retention policy. Where appropriate, organisations **should** seek legal advice.

a. Whether the offence casts doubt on the reputation of the individual and / or the organisation;

b. Whether the offence would affect an individual's ability to do the job;

c. Whether the conviction is relevant to the particular post. For example, a fraud related conviction could be problematic for a finance role;

d. The length of time since the offence happened;

e. The background and nature of the offence.

f. The seriousness of the offence;

g. Whether there is a pattern or history of offences.

Overseas Criminal Record Checks

62. The Disclosure and Barring Service, Disclosure Scotland and Access Northern Ireland are unable to access overseas criminal records. If, for this reason, insufficient evidence is provided by an unspent criminal records check with the relevant UK and Northern Ireland authorities, organisations **shall** obtain an overseas police record check. Guidance is available via:

a. Home Office

b. National Protective Security Authority (NPSA)

Reasons for concern and checking documentation

63. The BPSS process may uncover a number of factors which may, separately or in combination, raise concerns. Organisations **should** consider the following factors before offering employment:

    a. Involvement in illegal activities.

    b. False or unsubstantiated claims on a CV or application form.

    c. Unsubstantiated qualifications.

    d. Undeclared criminal convictions, particularly if they are revealed by other sources.

    e. Conflicts of interest from any secondary employment.

    f. Unexplained gaps in employment history.

    g. Negative, false or unresponsive references.

    h. Questionable documentation (for example, a lack of supporting paperwork or concern that documents are not genuine).

    i. Evasiveness or unwillingness to provide information on the part of the individual.

    j. Employment dismissals

64. If an individual's BPSS application is rejected, the organisation **shall** record the decisions and actions taken, and inform the individual of the outcome.

Additional Checks

Additional verification

65. BPSS checks are the baseline pre-employment checks for the UK government. National security vetting **shall** be considered if higher levels of assurance is required.

66. Organisations **shall**:

    a. Consult with the relevant teams, such as security, HR, legal and data protection teams, to confirm whether any additional checks are proportionate and lawful.

    b. Communicate any additional checks to individuals, for example in the organisation's privacy notice.

Post Verification

Recording checks and results of the BPSS

67. Organisations **shall:**

    a. Securely retain accurate and up-to-date BPSS records using the BPSS Verification Record (Annex B). The document is the official record of the successful completion of BPSS checks.The BPSS Verification Record **should** be shared appropriately when an individual's BPSS status needs confirming during a transfer or NSV application.

    b. Advise individuals to declare any changes in their personal circumstances under the Civil Service Code or local organisational policy, which could affect their role, for example a criminal conviction.

Reviewing the BPSS

68. BPSS does not have a validity period. Organisations **should** not need to review the BPSS checks once they have been passed, unless an individual:

    a. Transfers to another organisation, see **Joiners and Movers** section.

    b. Returns after a break in service over 12 months.

    c. Has a limited entitlement to remain in the UK.

        i. Organisations **shall** check if individuals' RTW status needs to be renewed before it expires.

    d. Declares, or is reported to have, a change in personal circumstances, see paragraph 67b.

69. Organisations **may** not need to conduct full BPSS checks when reviewing one aspect of an individual's BPSS, for example when an individual's RTW needs reviewing.

70. Organisations **can** decide, in line with their risk threshold, if an individual's BPSS needs reviewing if they have not started within six months after completing full BPSS checks.

71. Security teams **shall** be contacted if concerns are raised regarding an individual who has passed BPSS checks. As BPSS is a pre-employment check it cannot be withdrawn, however risks need to be mitigated to protect and safeguard organisational assets and individuals.

Annex A - Examples of acceptable identity documentation for BPSS

This **is not** a definitive list of acceptable identity documentation for the BPSS. Organisations **can** review other documentation in line with their risk appetite.

Organisations **should** check with the relevant criminal record agency for specific identification document requirements and for any further information if required: Disclosure and Barring Service (DBS (England and Wales)), Disclosure Scotland and AccessNI. Acceptable right to work documentation can be found on GOV.UK.

Group A – Original documents	**Group B** – Physical or digital documents issued within the past six months (name and current address within the document)
Valid passport	Mortgage statement containing current address
Valid driving licence (full or provisional) UK, Isle of Man and Channel Islands only.	Financial statement containing current address. This includes bank and credit card statements.
Birth certificate	Utility bill - for example energy, water, landline telephone or broadband (excluding mobile phone bills).
Marriage certificate	
National Insurance Number (NINO): These can be acquired fraudulently and cannot be relied upon as a sole means of establishing identity or right to work.	
Current evidence of Department for Work and Pension benefits.	
Recent HMRC tax notification (including online HMRC PAYE)	
Adoption certificate	
Divorce, dissolution or annulment papers.	

Civil Partnership certificate	
Recent council tax statement	

Annex B - Baseline Personnel Security Standard Verification Record

1. Employee/Applicant details

Surname:……..……
Forenames:……....

Address:…….…….....

Tel No: ……..……..

Date of birth:…….…
Place of birth:……...……...

Nationality:……
Former or dual nationality:……
(with dates if applicable)

2. Certification of identity

Document: Date of issue:

a.……
……

b.……...
……

c.……
……

d.……
…….....

3. References (if taken)

a.Referee:…….

Relationship:……..

Address:…….

Length of association:……

b.Referee:…….

Relationship:……..

Address:……

Length of association:……

c.Referee:……..

Relationship:……..

Address:…….

Length of association:……

4. Other information (this should include: verification of employment history (past three years); verification of nationality and immigration status, whether and when such immigration status needs to be rechecked and by whom; disclosure of unspent criminal record; academic certificates seen;

5. Any additional checks carried out:

I certify that in accordance with the requirements of the Baseline Personnel Security Standard:

I have personally examined the documents listed above and have established the identity of the named individual.

I have obtained the references (if taken) and information listed above and can confirm that these satisfy the requirements.

Name:……..

Job Title:……...

Signature:……..

Date:……

Annex C - Policy Document History

SPF Version	Document Version	Date published	Summary of Changes
1.0	1.0	Dec 2008	N/A
2.0	2.0	May 2009	Version 2.0 of the guidance reflects the Official Committee on Security, Sub-Committee on Personnel Security (SO(PS)) decision that full implementation of the BPSS (including application of the 'unspent' criminal record check on all recruits) is a core mandatory requirement of the SPF (MR23). Additional references to expert advice on immigration, nationality and right to work legislation and overseas criminal record checks have been incorporated.
3.0	2.1	Oct 2009	Version 2.1 of this guidance makes more explicit reference to Mandatory Requirement 23 and the removal of the reference to the document 'Identity Fraud – The UK Manual.' This version also advises that as a **pre-employment** screening process, we do not expect the BPSS to be applied retrospectively where assurances have already been obtained or are in place to allow for access to government assets.
5.0	3.0	February 2011	Version 3.0 of this guidance amends an erroneous reference to the List X 'Approval for Access' process and has been amended to reflect recent policy changes to reviews and renewals of the BPSS. Reference is also made to the Home Office's plans to review the Notifiable Occupation Scheme.
8.0	3.1	April 2012	Change to HMRC's address in Part II, paragraph 36 for checks on an employment record.
10.0	3.2	April 2013	Minor changes to format and branding. Updated links and contact details.
11.0	3.3	October 2013	Minor changes to formatting. Reference to HMRC Record Check removed and replaced with Civil Service Resourcing Employment History Check.

			National Insurance Number (NINO) Prefix list removed.
N/A	4.0	April 2014	Version 4.0 has been aligned to the new government classification policy for implementation in April 2014. Minor updates (e.g. to website links) are also included. The reference to the BPSS CD-Rom has been removed, as the content is out of date.
	5.0	January 2018	Version 5.0 reflects the introduction of the Disclosure Barring Service taking over from Disclosure Scotland for conducting unspent criminal record checks in England and Wales.
	6.0	June 2024	Language aligned with the Government Functional Standards. Improved clarity, formatting and removed outdated references. Organisations are now required to conduct Criminal Record Checks (unspent) as part of BPSS and not rely on NSV data.

Any enquiries regarding this publication should be sent to gsg-persecpolicy@cabinetoffice.gov.uk.

You can download this publication from GOV.UK.