Schedule 2.6 - Authority Policies

Index of Authority Policies

1 Part 1 – Sustainable Development Requirements

2 Part 2 – Life Chances

3 Part 3 – Welsh Language Scheme

4 Part 4 – Business Continuity Policy

5 Part 5 – Outline Job Description For Emergency Coordinator Officer

6 Part 6 – DWP Financial Authorities

7 Part 7 – DWP Records Management Policy

8 Part 8 – NOT USED

9 Part 9 – NOT USED

10 Part 10 – NOT USED

11 Part 11 – NOT USED

12 Part 12 – DWP Enterprise Security Risk Management Strategy

13 Part 13 – DWP Information Security Policy

14 Part 14 – DWP Off Shoring Policy

15 Part 15 – DWP Lone Working Risk Assessment Policy

16 Part 16 – DWP End of Day Process Guidance Note

17 Part 17 – DWP Health and Safety Policy

18 Part 18 – NOT USED

19 Part 19 – Unacceptable Customer Behaviour Policy

20 Part 20 – Small / Medium Enterprise Policy

21 Part 21 – Common Civil Service Pass Guidance

Part 1 – Sustainable Development Requirements

This Part sets out the "Sustainable Development Requirements" which are applicable to the provision of the Services.

1 General

1.1 The Supplier acknowledges that the Authority must at all times be seen to be actively promoting Sustainable Development through its environmental, social and economic responsibilities.

1.2 In delivering the Services, the Supplier shall and shall ensure that its Sub-contractors assist and cooperate with the Authority, by fully complying with the requirements of this Part.

2 Compliance

2.1 The Supplier shall produce a "Sustainable Development Policy Statement" and "Sustainable Development Plan" in accordance with paragraphs 2.2 and 2.3 of this Part, within 6 (six) months of the Effective Date and every 12 months thereafter. The Sustainable Development Policy Statement and Sustainable Development Plan must be specific to the Agreement and include all Sub-contractors involved in delivery for or on behalf of the Supplier. The Supplier must obtain the required information from Sub-contractors and then collate and submit as stated above.

2.2 In delivering the Services, the Supplier shall prepare a Sustainable Development Policy Statement giving, for each organisation involved in delivery of the contract an overarching commitment to:

a) dispose of contract waste in a legal manner (i.e. waste is disposed of via a registered waste collector, the Waste Electrical and Electronic Equipment (WEEE) regulations are adhered to where relevant);
b) reduce energy consumption;
c) promote waste management including recycling;
d) promote green or public transport;
e) promote Corporate Social Responsibility (CSR);
f) the Sustainable Development Policy and that of continuous improvement which should be signed and dated by senior management.

2.3 In delivering the Services, the Supplier shall prepare and deliver a Sustainable Development Plan which should be used to turn the commitment shown in the Sustainable Development Policy into action and which as a minimum, detail how each organisation involved in delivery of the contract will:

a) reduce their **Environmental** footprint of this contract through:

(i) minimising the use of energy, water and materials;
(ii) minimising waste and increasing recycling levels;
(iii) utilising recycled goods within operations;
(iv) providing efficient low carbon delivery methods;
(v) promoting the use of green or public transport.

b) contribute to **Social** sustainability of this contract through compliance with "Schedule 2.6 – Part 2 – Life Chances" where requested by the Authority.

c) drive **Economic** sustainability of this contract through:

(i) supporting job creation both locally and nationally;
(ii) facilitating opportunities for Minority Owned Businesses and Small and Medium-sized Enterprises.

2.4 To aid the department in monitoring the progress of each organisation the following information should also be included in your plan:

a) a baseline assessment of current position in terms of waste minimisation, recycling and energy consumption (energy consumption only required if current energy usage is available to organisations);
b) annual estimates of the progress of Sustainable Development actions;
c) details of how Supplier Personnel awareness of sustainability will be increased in line with the Sustainable Development Plan.

Part 2 – Life Chances

1 General

1.1 The Supplier acknowledges that the Crown is committed to assisting people to move from welfare to employment and driving forward improvements in economic, social and environmental well-being.

1.2 The Supplier (a) acknowledges that the Authority has a responsibility to support and promote wider social sustainability objectives for the benefit of society; and (b) agrees to cooperate with the Authority to improve life chances for those most disadvantaged and furthest from the labour market.

1.3 The Supplier acknowledges that the Authority is supporting the Crown's Life chances and social value agendas by aiming to promote opportunities for groups of persons ("**DWP Priority Groups**") which the Authority regards as meriting priority assistance including but not limited to apprentices, disabled people, young people, older workers, ex-offenders and black and minority ethnic people.

2 Diversity and Equality Delivery Plan

2.1 In addition to complying with its obligations set out in this Part, the Authority requires the Supplier to provide such information as the Authority may request on (a) the action(s) the Supplier is taking in the course of supplying the Services to comply with its obligations set out in this Part and (b) the effect such action(s) have on the Supplier Personnel used in the performance of its obligations under the Agreement.

2.2 As part of the information to be provided by the Supplier under paragraph 2.1 of this Part, the Authority requires the Supplier to provide to the Authority a diversity and equality delivery plan ("**Diversity and Equality Delivery Plan**") six (6) Months after the Effective Date, and annually thereafter. The Diversity and Equality Delivery Plan must be specific to the Agreement and include details of all Supplier Personnel including but not limited to all Sub-contractors involved in the performance of the Supplier's obligations under the Agreement, details of the action(s) the Supplier is taking to support the Crown's social value agenda including but not limited to the action(s) the Supplier is taking to meet its obligations under paragraph 2.3 of this Part.

2.3 The Supplier shall, and shall ensure that its Sub-contractors, take the following action(s) in respect of DWP Priority Groups:

a) Apprentices

- Ensure that (5) % of the Supplier Personnel used in the performance of the Supplier's obligations under the Agreement are apprentices.
- Make available to potential members of the Supplier Personnel used in the performance of the Supplier's obligations information about the National Apprenticeship Service.

b) Disabled People

- Take steps to become a Disability Confident Employer.
- Make appropriate use of Access to Work to support recruit and retain disabled workers.
- When recruiting Supplier Personnel to be used in the performance of the Supplier's obligations under the Agreement, offer disabled people interviews under a guaranteed interview scheme for vacancies for Supplier Personnel where the disabled people meet the minimum criteria for such vacancies.
- Offer work trials to disabled people to support filling vacancies for Supplier Personnel.
- Provide employment experience to disabled people as members of the Supplier Personnel used in the performance of the Supplier's obligations under the Agreement to develop their skills and experience and increase their employability.

c) Young People – Under 25

- Offer work trials to young people to support filling vacancies for Supplier Personnel.
- Provide employment experience to young people as members of the Supplier Personnel used in the performance of the Supplier's obligations under the Agreement to develop their skills and experience and increase their employability.

d) Older Workers – Over 50

- Offer work trials to older workers to support filling vacancies for Supplier Personnel.
- Provide employment experience to older people as members of the Supplier Personnel used in the performance of the Supplier's obligations under the Agreement to develop their skills and experience and increase their employability.

e) Ex-Offenders

- Offer work trials to ex-offenders to support filling vacancies for Supplier Personnel.
- Provide employment experience to ex-offenders as members of the Supplier Personnel used in the performance of the Supplier's obligations under the Agreement to develop their skills and experience and increase their employability.

f) Black and Minority Ethnic People

- Offer work trials to black and minority ethnic people to support filling vacancies for Supplier Personnel.
- Provide employment experience to black and minority ethnic people as members of the Supplier Personnel used in the performance of the Supplier's obligations under the Agreement to develop their skills and experience and increase their employability.

g) Employee Vacancies

- Advertise all vacancies for Supplier Personnel via Universal Jobmatch in addition to any other recruitment agencies with whom the Supplier advertises such vacancies and any other actions the Supplier takes to recruit Supplier Personnel.

2.4 The Diversity and Equality Delivery Plan must also include:

(a) an overview of Supplier and any Sub-contractor's policies and procedures for preventing unlawful discrimination and promoting equality of opportunity in respect of:

i) age;
ii) disability;
iii) gender reassignment;
iv) marriage and civil partnership;
v) pregnancy and maternity;
vi) race;
vii) religion or belief;
viii) sex; and
ix) sexual orientation.

(b) an overview of Supplier and any Sub-contractor's policies and procedures covering:

i) harassment
ii) bullying
iii) victimisation
iv) Supplier Personnel training and development

(c) details of the way in which the above policies and procedures are, or will be (and by when), communicated to Supplier Personnel;

(d) details of what general diversity and equality related training has been, or will be delivered (and by when), to Supplier Personnel;

(e) details of what structure and resources are currently directed towards active promotion of diversity and equality within the Supplier Personnel used in the performance of the Supplier's obligations under this Agreement, or if not currently in place, what will be put in place and by when;

2.5 The Authority will consider and must agree the contents of Diversity and Equality Delivery Plan. Any issues will be raised with the Supplier by the contract manager acting on behalf of the Authority. If an issue relates to a Sub-contractor, the Supplier must raise and resolve the issue with the Sub-contractor.

Life Chances Workforce Monitoring Template

2.6 The Supplier shall provide the Life Chances Workforce Monitoring template (contained in Appendix 1 to this Part), duly completed in full by the Supplier in respect of all Supplier Personnel (including but not limited to all Sub-contractors used in the performance of the Supplier's obligations under the Agreement), six (6) Months after the Effective Date and annually thereafter.

2.7 The Supplier shall complete the Life Chances Workforce Monitoring template in line with the 'Life Chances through Procurement Guidance for DWP Contractors'.

2.8 The Supplier will compare figures in all categories listed in the Appendix 1 - Workforce Monitoring template and provide (where possible) comparisons against any official national/regional statistics that are publicly available in accordance with the 'Social Value Guidance for Contractors' provided by the Authority to the Supplier.

2.9 The 'Social Value Guidance for Contractors' provides links to a number of data collection sources; this is not an exhaustive list and other sources are available. The Authority recognises that there may be regional variations in terms of population demographics and some data categories and coverage may not be complete or fully aligned, however, the Supplier agrees to provide high level analysis and identification of trends as and when requested by the Authority.

2.10 The Supplier shall provide and shall ensure that its Sub-contractors provide such evidence as the Authority may require of action(s) undertaken or planned by the Supplier and/or any Sub-contractor to improve the numbers in the Social Value Workforce Monitoring template (contained in Appendix 1 to this Part) to the satisfaction of the Authority.

2.11 Diversity and Equality, the Crown's social value agenda and DWP Priority Groups will be discussed jointly by the Authority and the Supplier as an on-going item at contract review meetings. Such meetings will discuss the information provided by the Supplier in accordance with paragraph 2.2 of this Part.

PART 2 - Appendix 1 – Life Chances Workforce Monitoring Template

Important – the figures the Supplier provides must relate specifically to the Supplier Personnel **used in the performance of the Supplier's obligations under the contract only, which for the avoidance of doubt includes any Sub-contractor.**

Name of Agreement:	
Contract Number:	
Name of Contractor:	
Effective Date:	
Total Number of Supplier Personnel**, which for the avoidance of doubt includes any Sub-contractors**	

1 – Number of new Supplier Personnel **posts created in the performance of the Supplier's obligations under the Agreement**

New Supplier Personnel **Posts**	**Number of new** Supplier Personnel **posts created in period**	
	1-34 hr per week posts	**35 hr + per week posts**
Baseline return (at 6 months for months 0-6)		
1st annual return (at 18 months for months 7-18)		
2nd annual return (at 30 months for months 19 - 30)		
3rd annual return (at 42 months for months 31-42)		

2 – Number of apprentices in Supplier Personnel **used in the performance of the Supplier's obligations under the Agreement**

DWP Priority Group - Apprentices	**Number of apprentices in** Supplier Personnel **which have been employed for 26 weeks or longer in period**	**% of apprentices in** Supplier Personnel **at the end of the period**	**Number of apprentices who began apprenticeships as part of the** Supplier Personnel **during the period**
Baseline return (at 6 months for months 0-6)			
1st annual return (at 18 months for months 7-18)			
2nd annual return (at 30 months for months 19 - 30)			
3rd annual return (at 42 months for months 31-42)			

3 – Number of disabled people in Supplier Personnel **used in the performance of the Supplier's obligations under the Agreement**

DWP Priority Group - Disabled People	**Number of disabled people in** Supplier Personnel **which have been employed for 26 weeks or longer in period**	**% of disabled people in** Supplier Personnel **at end of period**	**Number of disabled people who began employment as part of the** Supplier Personnel **during the period**
Baseline return (at 6 months for months 0-6)			
1st annual return (at 18 months for months 7-18)			
2nd annual return (at 30 months for months 19 - 30)			
3rd annual return (at 42 months for months 31-42)			

4 – Number of disabled people, who had been interviewed by the Supplier under the Guaranteed Interview Scheme (GIS) for Supplier Personnel **posts used in the performance of the Supplier's obligations under the Agreement.**

DWP Priority Group – disabled people in the Supplier Personnel **who had been interviewed by the Supplier under the GIS**	**Number of disabled people who have been interviewed for** Supplier Personnel **posts by the Supplier under the GIS during the period**
Baseline return (at 6 months for months 0-6)	
1st annual return (at 18 months for months 7-18)	
2nd annual return (at 30 months for months 19 - 30)	
3rd annual return (at 42 months for months 31-42)	

5 – Number of young people in Supplier Personnel **used in the performance of the Supplier's obligations under the Agreement**

DWP Priority Group - Young People	**Number of young people in** Supplier Personnel **which have been employed for 26 weeks or longer in period**	**% young people in** Supplier Personnel **at end of period**	**Number of young people who began employment as part of the** Supplier Personnel **during the period**
Baseline return (at 6 months for months 0-6)			
1st annual return (at 18 months for months 7-18)			

2nd annual return (at 30 months for months 19 - 30)			
3rd annual return (at 42 months for months 31-42)			

6 – Number of older workers in Supplier Personnel **used in the performance of the Supplier's obligations under the Agreement**

DWP Priority Group - older workers	**Number of older workers in** Supplier Personnel **which have been employed for 26 weeks or longer in period**	**% older workers in** Supplier Personnel **at end of period**	**Number of older workers who began employment as part of the** Supplier Personnel **during the period**
Baseline return (at 6 months for months 0-6)			
1st annual return (at 18 months for months 7-18)			
2nd annual return (at 30 months for months 19 - 30)			
3rd annual return (at 42 months for months 31-42)			

7 – Number of ex-offenders in Supplier Personnel **used in the performance of the Supplier's obligations under the Agreement.**

DWP Priority Group - ex-offenders	**Number of ex-offenders in** Supplier Personnel **which have been employed for 26 weeks or longer in period**	**% ex-offenders in Supplier Personnel at end of period**	**Number of ex-offenders who began employment as part of the** Supplier Personnel **during the period**
Baseline return (at 6 months for months 0-6)			
1st annual return (at 18 months for months 7-18)			
2nd annual return (at 30 months for months 19 - 30)			
3rd annual return (at 42 months for months 31-42)			

8 – Number of black or minority ethnic people (BME) in Supplier Personnel **used in the performance of the Supplier's obligations under the Agreement.**

DWP Priority Group - black or minority ethnic people	**Number BME in** Supplier Personnel **which have been employed for 26 weeks or longer in period**	**% BME in** Supplier Personnel **at end of period**	**Number of BME who began employment as part of the** Supplier Personnel **during the period**
Baseline return (at 6 months for months 0-6)			
1st annual return (at 18 months for months 7-18)			
2nd annual return (at 30 months for months 19 - 30)			
3rd annual return (at 42 months for months 31-42)			

9 – Number of Employment Experience placements conducted in the performance of the Supplier's obligations under the Agreement

Employment Experience placements	**Number of Employment Experience placements conducted during the period**
Baseline return (at 6 months for months 0-6)	
1st annual return (at 18 months for months 7-18)	
2nd annual return (at 30 months for months 19 - 30)	
3rd annual return (at 42 months for months 31-42)	

10 – Number of Work Trials conducted as part of the recruitment of Supplier Personnel used in the performance of the Supplier's obligations under the Agreement.

Work Trials	**Number of Work Trials conducted during the period**
Baseline return (at 6 months for months 0-6)	
1st annual return (at 18 months for months 7-18)	
2nd annual return (at 30 months for months 19 - 30)	
3rd annual return (at 42 months for months 31-42)	

11 – Number of vacancies for Supplier Personnel advertised via Universal Jobmatch

Supplier Personnel vacancies advertised via Universal Jobmatch	**Number of vacancies for Supplier Personnel advertised via Universal Jobmatch during the period**	**% of all vacancies for Supplier Personnel advertised via Universal Jobmatch during the period.**
Baseline return (at 6 months for months 0-6)		

1st annual return (at 18 months for months 7-18)		
2nd annual return (at 30 months for months 19 - 30)		
3rd annual return (at 42 months for months 31-42)		

Part 3 – Welsh Language Scheme

This Part sets out the Supplier's obligations which are applicable to the provision of the Services in Wales.

1 General

1.1 The Supplier acknowledges that in relation to the operation of its Services which are delivered in Wales, the Authority must at all times be seen to be actively promoting the equality of the English and Welsh languages, in accordance with the Welsh Language Act 1993.

1.2 In the performance of the Agreement, the Supplier shall ensure that it cooperates with the Authority in satisfying this duty, by fully complying with the requirements of this Part.

2 The DWP Welsh Language Scheme

2.1 The DWP Welsh Language Scheme can be found at:

https://www.gov.uk/government/organisations/department-for-work-pensions/about/welsh-language-scheme

2.2 The Supplier shall, in the delivery of the Services, ensure that it complies with the Department for Work and Pensions Welsh Language Scheme and such instructions as the Authority may issue from time to time in respect of promoting the equality of the English and Welsh languages.

3 Delivery of Services Through the Medium of Welsh

3.1 The Supplier undertakes that those who have dealings with them are able to do so in English or Welsh, whichever is their preference.

3.2 The Supplier will ensure that:

a) those who want, or are required, to correspond with the Supplier will be able to do so in English or Welsh;

b) those who are known to prefer corresponding through the medium of Welsh will have correspondence initiated in Welsh;

c) any correspondence received in Welsh will be answered in Welsh within the same timescales and standards as those written in English;

d) staff who are in Wales will greet any telephone callers in English and Welsh until the caller's preferred language can be ascertained;

e) any help lines set up to deliver the service must offer a Welsh or English option and sufficient Welsh language speakers must be available to deal with callers through the medium of Welsh, if they select the Welsh option;

f) any answer phones in the Supplier's offices in Wales will have a pre-recorded bilingual message;

g) all people who participate in the Services are able to contribute through the medium of English or Welsh;

h) all material published and printed for use in Wales shall be available in English and Welsh, and available for use within the same timescales. The standard of bilingual or Welsh material shall be of equal quality to those produced solely in English;

i) all forms and explanatory material be available in both English and Welsh and available for use within the same timescales; and

j) any complaints or grievance procedure should be provided in both English and Welsh.

k) any websites, including any interactive pages, set up to support the delivery of the service must be available in both Welsh and English;

l) where DWP has notified the Supplier or the participant has identified that Welsh is their preferred language this should be recorded, ensuring all future dealings with that participant will be in Welsh.

Part 4 – Business Continuity Policy

Introduction

DWP is the UK's biggest public service department, with the responsibility for delivering services to some of society's more vulnerable people, so it is vital that we continue to meet our business objectives, obligations and statutory duties. Robust business continuity planning is therefore essential to ensure that DWP can respond promptly and effectively to any form of disruption, so as to minimise the adverse effect on delivery of our services.

DWP follows the Business Continuity Institute's Lifecycle and Professional Practices which are aligned to the internationally-recognised industry standard for Business Continuity Management - ISO22301. This sets out the types of controls, procedures and best practice that organisations can adopt.

Links to guidance referred to in the policy are shown at the end of the document.

Policy and programme management

It is mandatory, throughout DWP, to follow the business continuity management (BCM) arrangements set out in this policy and in our other guidance documents. To ensure a standard approach across all parts of DWP, business continuity is managed centrally by the DWP Continuity & Resilience Team (C&RT) – formerly the Business Continuity Team.

Principles of business continuity management in DWP

The principles of BCM within DWP are:

- BCM is undertaken to benefit DWP and its customers by providing resilience in times of disruption
- The highest level of accountability for BCM sits with the Departmental Continuity and Resilience Director
- Each Director General or Operations Directorate within DWP has a Continuity and Resilience Director
- All managers are responsible and accountable for BCM within their area, with the support of their Continuity and Resilience Team Business Partner
- BCM must be considered within the processes for managing and implementing change
- Disruptions to service (regardless of cause) are managed at the lowest appropriate level within the organisation. Incidents are only escalated if the consequences of the disruption cannot be managed at this lower level
- Our arrangements are subject to review by Internal Audit.

Business continuity management standards in DWP

The BCM standards which DWP adheres to are:

- All operational sites and Director Generals must have Business Continuity Plans (BCPs) which follow the relevant templates provided by C&RT. Other levels within the organisation (for example Divisions, teams) may not need BCPs, depending on the critical nature of the

service(s) they deliver, but must, as a minimum, have a strategy in place for communication cascades to key contacts

- BCPs must be reviewed following a change to business processes, or after use for a disruption or exercise. The local content must be reviewed at least quarterly to ensure contact details, skills and travel information are kept up-to-date.
- BCPs must be exercised at least once a year unless they are tested by being used for an actual disruption. The C&RT will review the lessons learned from the disruption and judge whether the disruption sufficiently tested the plan or if an annual exercise is still needed.
- An assessment of the lessons learned must be undertaken following any business continuity exercise or actual disruption that has resulted in the use of the BCP
- If areas for improvement are identified as a result of lessons learned these must be implemented or escalated to C&RT to consider whether there is a wider impact
- C&RT will undertake work throughout the year to assure all BCPs are fit for purpose and will provide support where any improvements are identified
- All individuals must be aware of BCPs which affect their site/business area and should ensure they fully understand their role and responsibilities in the event of a disruption
- DWP induction processes and materials for new starters must include guidance about business continuity
- Suppliers are required to have BCPs, which meet DWP requirements, to ensure any disruption to their service has minimal impact on DWP services
- C&RT will work with IT colleagues and suppliers to agree and achieve acceptable recovery time objectives
- All change projects/programmes must consult the C&RT from the start to ensure compliance with policy.

Structure for managing business continuity

DWP has a formal structure for managing BCM, with associated responsibilities.

Business continuity roles in DWP

The key business continuity roles in DWP are:

- Departmental Continuity & Resilience Director who reports to the Permanent Secretary and is accountable to the Executive Team and the Departmental Board for ensuring robust business continuity arrangements are in place
- The Head of Security Policy, Assurance and Resilience Division sets and drives the overall vision and strategy linking security and business continuity
- The Head of Continuity & Resilience leads the C&RT, setting the strategic direction and engaging across DWP and across Government
- Two Continuity & Resilience Managers are responsible for the work of the C&RT, support the Departmental Continuity & Resilience Director and are available at all times to manage any major disruption

- C&RT are DWP's business continuity experts and are responsible for delivering the BCM programme for DWP using a business partner model. This includes:

    - Raising awareness of BC and embedding best practices
    - Identifying threats and risks for the business and developing contingency plans to minimise disruption
    - Assuring robust BCPs are in place and are exercised
    - Providing guidance on all aspects of BCM
    - Managing major disruptions, where delivery of national service is affected or that cannot be managed at a local level
    - Liaising across Government to provide input from DWP on planning, exercises and intelligence gathering

- In addition, each Director General will have a nominated Continuity & Resilience Director, accountable to the DWP Executive Team for business continuity within their area.

- The Continuity and Resilience Board brings together these Continuity & Resilience Directors to consider high level threats and risks and agree required actions.

Embedding

DWP C&RT, along with all managers, is responsible for raising awareness of business continuity and embedding BCM practices. It is important that BC is embedded into projects and programmes from the beginning to ensure that BC is part of the change culture.

DWP induction processes and materials for new starters must include guidance about business continuity.

Information and awareness of BCM can be gained through a number of routes:

- BC intranet site

- Assurance visits

- Exercising plans

- Briefings for new managers/coordinators

- Induction for new members of staff.

Business continuity training for all staff is available on the Civil Service Learning website and provides staff with an overview of what business continuity is, and the benefits of having effective business continuity management in place. (More information about this is available on the BC intranet site).

C&RT members will follow the Professional Pathways for the Security Policy, Assurance and Resilience Division, including specialist training as appropriate.

DWP also participates in the annual international Business Continuity Awareness Week, taking the opportunity to highlight BCM to all colleagues in DWP.

Analysis (understanding the organisation)

DWP C&RT has a key role in understanding how our key products and services could be disrupted, assessing the impact of such a disruption and developing contingencies to minimise the effects. To make this assessment the C&RT completes a business impact analysis (BIA) for each key service.

The purpose of a BIA is to:

- Identify points of failure
- Document the impacts over time that would result from a disruption
- Identify the maximum tolerable period of disruption or outage – the time it would take for adverse impacts to become unacceptable
- Establish the recovery time objective – the period of time following an incident within which an activity/service must be resumed
- Determine the priorities for recovery.

A BIA helps us to identify our dependence on individual IT systems, processes or suppliers/partners. This can help with the management of disruptions and contracts.

Any risks identified through completing or reviewing the BIA will be captured on the BCT Risk Register and escalated to relevant stakeholders.

Design (developing strategies)

DWP C&RT is responsible for working with subject experts to produce business continuity guidance for a range of services, systems or threats (such as Industrial Action). Guidance is available on the BC website.

As well as bespoke guidance there are standard mitigations which can be used.

Loss of people

- Multi-skill individuals to ensure key roles are covered
- Document key processes
- Spread the workforce geographically.

Loss of premises

- Use twinning arrangements – diverting customers, staff or work
- Displace some people to accommodate those doing work of a more immediate priority.

Loss of technology or suppliers

- Ensure contracts with external providers contain appropriate business continuity clauses.

Implementation

DWP has a well-rehearsed, flexible and tiered incident response structure which can be activated at very short notice. The key elements of the response structure are the:

- DWP BCP
- Incident management roles and forums
- Communications strategy, including regularly maintained key contacts lists.
- DWP BCP and supporting guidance describes the Department's response to known threats and risks, including:
- Loss of IT
- Industrial action
- Severe weather
- Pandemic health disruption.

Minor disruptions occur regularly and these are handled, as part of normal business, at the most appropriate level using that site/business area's BCP. A disruption to, or loss of service, should be reported to the C&RT Northern or Southern Hub or the relevant Business Partner so they can provide support. The business continuity guidance on managing a disruption explains the incident management process and the support available for any area of DWP which is affected by disruption. This is backed up by specific BC guidance for key products and services.

C&RT's communications approach includes issuing messages to affected parts of the business explaining the issue and providing guidance. This will generally be by e-mail but may also be through SMS text message or using the Staff Emergency Information Line and emergency internet and intranet sites. C&RT will work with other colleagues to provide briefings and press lines as required.

Disruption Forums (DF)

Where an incident cannot be managed in the usual way because the effect is too great then the C&RT will convene a Disruption Forum (DF).

There are three levels of Disruption Forum:

- Operations Disruption Forum (ODF) – chaired by C&RT Manager and called when there is a need for a business level discussion about contingencies which might be deployed
- Business Disruption Forum (BDF) – chaired by the Departmental Continuity & Resilience Director and called when there is a major disruption which is significantly affecting customer service and which can't be managed at the lower level. The disruption may be DWP-wide or wholly/mainly in Operations
- Departmental Disruption Forum (DDF) – a meeting of ET, chaired by the Departmental Continuity & Resilience Director, which is called only in the event of a high level disruption, such as a terrorist threat or an acute failure of IT

There may be times when all levels will operate together, with the DDF providing the executive steer, the BDF managing the disruption and the ODF working on the detail.

Disruption forums:

- Provide relevant expertise to inform discussions
- Direct management of the incident
- Mobilise resources
- Agree priorities
- Agree implementation of additional contingency measures.

C&RT will act as secretariat for any DF and issue actions and instructions as agreed.

Validation

C&RT undertakes a schedule of visits throughout the year to assure BCPs are fit for purpose. This process is validated to ensure consistent standards are being applied. Where any improvements are identified C&RT will help the BCP owner to develop and implement an action plan. The guide to assurance gives full details.

To maintain effectiveness, as well as being subject to the above assurance, business continuity arrangements should be reviewed and exercised regularly.

The guidance on exercising plans explains how this can be done. C&RT will work with BC leads to exercise Director General-level plans and may provide support with site exercises.

DWP takes part in cross-government business continuity exercises arranged by the Civil Contingencies Secretariat (Cabinet Office). Our involvement depends on the scenario being tested. Participation ensures DWP interests are taken into account and strengthens cross-government working relationships.

Further information

For further information please see the Business Continuity intranet site, including the following areas:

Assurance

BC products and guidance homepage

DWP Business Continuity Plan

Guide for projects

Exercising your business continuity plan

Part 5 – Outline Job Description for Emergency Coordinator Officer and Incident Control Officer

The ECO is responsible for:

- Acting as the focal point during a fire or bomb evacuation
- Confirming that the Fire Brigade has been informed, and have been given details and location of the fire
- Liaising with the emergency services, ICO*, security guards, fire wardens and other key personnel
- Receiving reports from the fire wardens and other key personnel
- Ensuring that any employees/visitors/contractors who cannot be accounted for at the assembly point are reported to the Fire Brigade on their arrival
- Retaining copies of PEP summaries

*The ICO is responsible for:

- Working with the ECO to co-ordinate any evacuation
- Receiving reports from the ECO
- Disseminating information to staff and trade unions
- Acting as ECO when there is no ECO based on the site

Part 6 – DWP Financial Authorities

1 Delegated Financial Authority (also known as Delegated Purchasing Authority)

Delegated Financial Authority can be defined as a standing authorisation for an individual to incur expenditure in a single transaction, within prescribed limits and against specific account codes and cost centres, without prior HM Treasury or Budget Holder approval.

The assigning of transaction limits must be appropriate, based upon business needs, an individual's grade, the nature of their role, their skills and experience, and the volume and levels of transactions. Delegated Financial Authority should only be given to DWP staff.

DWPs systems require all requisitions and payment authority forms to be approved by a suitable person.

[Redacted]

2 Delegated Buying Authority

Delegated Buying Authority can be defined as authorisation to create or approve an individual Purchase Order to incur expenditure within prescribed limits and against specific account codes and cost centres.

Where formal contract documentation is in place and a PO supports this, approval of a PO is administrative and does not require DPA. Where no documentation is in place, the creation of a PO may form a contract. Users with the Purchasing Manager responsibility must be aware of this and ensure they do not approve a PO which, in effect, forms a contract which exceeds their DPA level.

[Redacted]

Part 7 – DWP Records Management Policy

[REDACTED]

Part 8 – NOT USED

Part 9 – NOT USED

Part 10 – NOT USED

Part 11 – NOT USED

Part 12 – DWP Enterprise Security Risk Management Strategy

[REDACTED]

Part 13 – DWP Information Security Policy

DWP_TOM_Schedule
02.6_Authority Policie

Part 14 – DWP Offshoring Policy

guide-for-dwp-...

Part 15 – DWP Lone Working Risk Assessment Policy

Lone Working Risk Assessment

1 Background and Legal Requirements

1.1 There are no specific health and safety regulations applicable to DWP people working alone, however under the Management of Health and Safety at Work Regulations (1999) employers have a general duty to identify hazards, assess all risks to health and safety and put measures in place to control those risks.

1.2 It follows that the potential hazards involved in working alone must be controlled by the application of the risk assessment process and it is an employer's duty to ensure their lone workers health and safety at work.

1.3 Lone workers may be defined as those who work by themselves without close or direct supervision. Within DWP this typically involves:

(a) Mobile workers working alone away from their fixed base. For example, meeting customers in their own homes or visiting employers/training providers;

(b) working alone within the normal place of work (for example, working alone because colleagues have yet to arrive or have already left for the day, working outside of normal working hours/overtime working).

Note: A lone workers risk assessment is not required when travelling alone.

1.4 Lone workers should not be more at risk than other employees. In order to achieve this through the risk assessment process, risk control measures additional to those applied to other work practices may be required.

1.5 There are a variety of measures that must be introduced in order to control these new risks. Among these are:

(a) suitable training to ensure competent individuals carry out the work;

(b) adequate supervision (for example, ensuring check in arrangements are in place);

(c) good communication systems between the line manager and the lone worker;

(d) careful planning of the lone working task;

(e) accident and emergency arrangements in place (including First Aid).

1.6 The procedures for arranging for a lone workers risk assessment to be carried out will vary depending on where the lone working takes place but the completed risk assessment will remain valid even where lone working occurs intermittently, provided a review is not otherwise required.

2 Procedures

Lone working in DWP buildings

2.1 Whenever it is intended that DWP staff are required to work alone in DWP buildings including, for example, when working outside normal working hours means they are left working alone, line managers should first review the proposed arrangements against the generic Lone Worker risk assessment contained in the Consolidated Risk Assessment Model (CRAM) at Annex A, for the site concerned. The CRAM is a risk assessment pack managed and maintained by the current FM Service Partner under the PRIME Contract.

2.2 They include consideration of:

(a) Evacuation procedures;

(b) First Aid and raising the alarm in the event of injury or illness;

(c) Use of equipment

(d) Risk of assault;

(e) Health problems and working alone;

(f) Unfamiliarity with surroundings;

(g) Line Managers' monitoring procedures; and

(h) Appropriate training, instruction, supervision and guidance for staff.

2.3 In the event of any queries about these generic controls, or in any situation where the generic controls do not appear to control the risks, Line Managers should contact their Facilities Manager for further competent advice.

2.4 Any other relevant personal risk assessments - for example New/Expectant Mothers, Young Persons - should be reviewed by the Facilities Manager.

2.5 Using risk assessment documentation, the risk assessor will arrange to meet the individual to gather the relevant information and carry out the risk assessment.

3 Lone Working Away from DWP Buildings

3.1 Where lone working takes place away from DWP buildings there are different arrangements in place. Line managers will be required to apply a model risk assessment approach to meet their legal responsibilities. Line managers are required to undertake the DWP training event 'Health and Safety Responsibilities for Managers' and this training will provide the background knowledge to assist them with this action.

3.2 A model risk assessment has been developed at Annex B Line managers are responsible for checking the model risk assessment to ensure that local circumstances are consistent with the contents.

3.3 The model risk assessment provides a comprehensive list of suitable and sufficient measures that will control the risks involved in lone working away from the office across a broad range of situations.

3.4 It does not address the particular hazards involved in activities such as home visiting or working in non DWP buildings. Separate guidance on these subjects may be found on the Occupational Health and Safety Division website.

3.5 A prompt sheet has been provided at Annex C to enable managers to identify health and safety issues to be considered and record any additional significant hazards not addressed by the model risk assessment.

3.6 When line managers identify the need for a lone workers risk assessment for off-site working they should:

(a) Read through and become familiar with the model risk assessment contents;

(b) check through the prompt sheet to ensure that all significant hazards have been identified and controlled by the model risk assessment;

(c) where additional significant hazards are identified or hazards recorded on the model risk assessment are not properly controlled, arrange for completion of a further lone workers risk assessment:

(d) discuss the findings of the risk assessment with the lone worker and agree the content;

(e) ensure the lone worker has a copy of the model risk assessment findings and prompt sheet (or completed risk assessment where appropriate).

3.7 Line managers must **always** discuss the findings and agree the content with each lone worker and ensure that they retain a copy of the risk assessment findings and prompt sheet (or completed risk assessment where appropriate).

3.8 Line managers must review the risk assessment (recording the review on the prompt sheet) to ensure that the control measures are still suitable and sufficient. Where it is considered they no longer apply arrangements should be made to carry out a further lone workers risk assessment.

3.9 Reviews must be carried out annually as a minimum or in the following circumstances:

(a) When conditions that significantly change the risks have occurred since the original risk assessment;

(b) within two days of a serious incident/accident;

(c) before a pilot and/or implementation of any new work practice is to be introduced that significantly changes the risks;

(d) following a reasonable request from the individual member of staff.

Part 16 – DWP End of Day Process Guidance Note

Guidance Note - End of Day Process

Following an unfortunate incident where a DWP member of staff died on site but remained undiscovered for a number of days due to the Bank holiday weekend, DWP have instigated a review of ‘End of Day’ processes to ensure that all individuals are accounted for once a site closes for the day.

Whilst the monitoring of DWP staff whereabouts will be the responsibility of the Client, there are activities that the Security Services Contractor undertake, which can assist DWP in ensuring staff have left site safely. Additionally we want to ensure that all staff including DWP, Contractors, Service Partner/other individuals have been accounted for prior to the building closing.

It is not the intention, as part of this review, to necessarily start introducing additional building checks by Security Service Contractor (e.g. additional/later patrols) but to consolidate the detail of what happens currently so that management arrangements can be implemented to ensure the safety of staff out with this.

Please note: Anything that may require additional actions by Security Service Partners (e.g. additional patrols, later opening, etc.) may require a commercial change (e.g. additional charge).

Part 17 – DWP Health and Safety Policy

Section A - DWP Health and Safety Serious Incident (Fast Track) Policy

Introduction

The Department's Health and Safety Serious Incident (Fast Track) Policy aims to set out the expectations for the reporting and review of incidents where a serious (or potentially serious) incident occurs which compromises the Health and Safety of DWP staff, visitors and partners.

Who does this Policy apply to?
This policy applies to anyone involved in ensuring the effective safety of DWP staff, visitors and partners, whether through the agreed Serious Incident (Fast Track) reporting system or managing any related actions and impacts.

Health and Safety Serious Incident (Fast Track) Definition
Incidents reportable under this policy are not defined by specific type such as "Actual Physical Assault" but will be defined by the following qualifying statement:

"A serious incident occurs, which compromises the health and safety of DWP staff or the staff of our Partners and/or our ability to safely use our premises. The serious nature or sensitivity of the incident warrants an immediate notification to senior management, prior to further investigation".

The Policy - What action will we take

Serious Incident Reporting

Part One: Fast Track Incident – Notification (FT1)

An agreed notification process is in place to ensure that all appropriate individuals including Senior Managers across all areas of DWP business receive the report form as timeously as possible. Where needed appropriate senior colleagues from our service providers will also be made aware of the incidents at the same time.

The notification should be completed as soon as possible following after the incident by the most appropriate individual (usually the site manager). It must:

- Provide site details and contact information
- It must be factual and as far as possible be a true and honestly held account of actions and information from the incident as understood at the time. This may include but not limited to feelings of those involved and any language used.
- It should not include individuals' names;

The information received will be recorded and used for statistical and analytical purposes – which may also be subject to Freedom of Information, Subject Access, Parliamentary Questions and any related legal proceeding requests.

Note: Fast Tracks may also be recorded on the department's Unacceptable Customer Behaviour (UCB) database where the actions recorded deem it necessary to do so. Where this occurs the database records will be annotated as such and a copy of the Serious Incident documents should be attached to the UCB record.

Part Two: Fast Track Incident – Review (FT2)

The aim of the review is to consider fully any factors that may have contributed to the root cause of the incident, and make appropriate recommendations to improve Health and Safety at all levels across the Department.

The Review process should as far as possible occur within 4 days of the Serious Incident occurring and will where available include reviewing CCTV footage in line with agreed Data Protection Principles.

The final review document will be agreed by all attending parties before issue to the agreed FT2 notification list.

The information received will be recorded and used for statistical and analytical purposes – which may also be subject to Freedom of Information, Subject Access, Parliamentary Questions and any related legal proceeding requests.

PART Three: Fast Track Incident - Recommendations (FT3)

Recommendations will be made as part of the Review Process and recorded as part of the associated documentation.

It is the responsibility of the site manager to ensure any recommendations are adhered to and followed up when action is not taken in line with the recommendation.

The Site manager will also ensure that the DWP Health and Safety Team is kept up to date in line with the latest “action by” date.

The DWP Health and Safety Team may contact the site manager for information and further updates where deemed necessary.

The information received will be recorded and used for statistical and analytical purposes – which may also be subject to Freedom of Information, Subject Access, Parliamentary Questions and any related legal proceeding requests.

Links to other policies
Unacceptable Customer Behaviour
Data Protection
Freedom of Information
Suicide and Self Harm

Review
Annually or sooner where legislation or significant change requires it.

Annex 2 – Fast Track One Incident Report Form

[REDACTED]

Annex 2 – Fast Track Two Incident Report Form

[REDACTED]

Section B - Call Handling and Jobcentre Claimant Facing Risk Assessments Review Process in PRIME Sites – A Framework for Managers

4 Introduction

4.1 This guidance sets out the DWP policy and procedures in place to review Call handling and Jobcentre Claimant Facing Risk Assessments (CHRA and JCFRA) in Authority sites.

4.2 DWP groups each have Health and Safety Business Partners whose duties include providing expert advice and support to their people to help them fulfil their health and safety responsibilities. Site Managers should contact their local Business Partner if they require further guidance when carrying out the review of the site CHRA and JCFRA.

5 CHRA and JCFRA Review Responsibilities

5.1 Senior Manager:

that a suitable and sufficient CHRA and JCFRA is in place, including satisfying themselves that the activities described in this guidance are carried out (they may not delegate this accountability to the Site Manager). The senior manager in Jobcentres will be the District Manager, and the Group Manager in CCD and BDC

5.2 Site Manager:

5.3 Ensuring that a suitable and sufficient CHRA and JCFRA and subsequent reviews are in place and recorded for each DWP site and stored online, there is no need for paper copies to be retained;

5.4 Providing information to enable the CHRA and JCFRA review to be carried out in partnership with the Risk Assessor where appropriate;

5.5 Ensuring the CHRA and JCFRA is reviewed when required;

5.6 Signing off the CHRA and JCFRA reviews;

5.7 Consulting with staff and TU Appointed Safety Representatives;

5.8 Ensuring the CHRA and JCFRA reviews are correctly recorded;

5.9 Ensuring control measures identified during the CHRA and JCFRA reviews have been implemented and continue to remain suitable and sufficient (e.g. adequate staffing levels, all necessary training, changes to Incident Management Plans) and also ensuring that the control measures that are the responsibility of the Security Services Provider (e.g. the number of CCO's, CCTV, escape routes) are suitable and sufficient. If there is any doubt a review of the Security Risk Assessment should be ordered via the Integrator helpdesk;

5.10 Ensuring staff are informed of the identified risks and control measures, including any revisions;

5.11 Ensuring that Control Measures Continue to Reflect Working Practices and Conditions;

6 The Risk Assessor (as the DWP Health and Safety Competent Person):

6.1 Will participate in reviews when a new activity may:

6.1.1 Impact on security arrangements and may require a review and revision of the Jobcentre Security Risk Assessment;

6.1.2 Relates to the building, including furniture, equipment, and the use of IT equipment and building fabric and services.

6.2 Will where appropriate work with the Site Manager to ensure the CHRA and JCFRA review is suitable and sufficient;

6.3 Will provide health and safety support to DWP when their technical expertise is required;

6.4 Will implement applicable control measures e.g. installing CCTV

7 DWP Estates:

7.1 Will provide advice and support to Managers on the contractual obligations of the Security Services Provider.

8 When Should the CHRA and JCFRA be Reviewed?

8.1 The CHRA and JCFRA must be reviewed annually as a minimum or:

8.2 When conditions have changed significantly since the time of the original assessment e.g. layout changes are proposed, new equipment is introduced, the pattern of accidents or assaults changes significantly;

8.2.1 Following a Fast Track incident

or

8.2.2 Unacceptable Claimant Behaviour related accident;

8.2.3 Before a pilot and/or implementation of any new work process or activity is to be introduced that significantly changes the risk;

8.2.4 When there are significant personnel changes.

Note: All these events must be considered against the CHRA AND JCFRA existing risk control measures for their effect on:

(a) Staff;

(b) Others, e.g. claimants and visitors;

(c) Security measures;

(d) Environmental aspects;

8.3 The CHRA and JCFRA may also be reviewed following a reasonable request from an individual member of staff, the Safety Committee representing the site or by a local Trade Union Appointed Safety Representative.

9 Preparing for the CHRA and JCFRA Review

9.1 The Site Manager will:

9.1.1 Consult with the Trade Union Appointed Safety Representative before the review of the CHRA and JCFRA takes place and invite them in good time to:

9.1.2 Raise any relevant issues in writing with the Site Manager before the review and any issues identified during the review of the CHRA and JCFRA should be put in writing after the review;

9.1.3 Attend and take part in the review of the CHRA and JCFRA.

9.1.4 Consult with external partner organisations where they are affected (e.g. when staff from an outside organisation are working in Authority premises).

9.1.5 Provide all necessary documentation to enable the CHRA and JCFRA review to be carried out for example:

(a) The CHRA and JCFRA;

(b) Business delivery and staffing level plans;

(c) Proposed/existing floor plans;

(d) Expected claimant volumes;

(e) Client groups (including numbers recorded on the Staff Protection List (SPL));

(f) Accident and incident records;

(g) Proposed/existing Incident Management Plans;

(h) Quarterly Inspection records.

(i) Workplace Risk Assessment

9.2 This list is not exhaustive. The documentation examined to inform the review of the CHRA and JCFRA will depend on local conditions. Site Managers should use the CHRA and JCFRA Review Prompt Sheets to help them identify areas to consider before and during the review of the risk assessment, relevant information should be transferred onto the prompt sheet which will be retained with the CHRA or JCFRA to inform future reviews / revisions. It will be for Site Managers to determine what documentation and information to bring to the risk assessment review, taking advice from the Risk Assessor and/or HSBP as necessary.

9.3 Site managers must ensure that all appropriate documentation is made available in advance of the risk assessment review.

10 Arranging the CHRA and JCFRA Review

10.1 Site Managers are responsible for undertaking an initial review in all cases using the current CHRA and JCFRA. At this stage the Risk Assessor will not normally be involved. If the site manager decides Authority Supply Chain members should be involved in the review they should contact the Integrator Helpdesk to arrange a date for review.

10.2 On receipt of this request the Risk Assessor will:

10.2.1 Contact the Site Manager (as required contractually within 20 working days) to agree a time and date to carry out the CHRA and JCFRA review (this date will be at least 10 working days ahead); and

10.2.2 Discuss with the Site Manager the documentation that should be gathered and be available at the review of the CHRA and JCFRA.

11 Completing the CHRA and JCFRA Review

11.1 The JCFRA will be completed by DWP sites who deal with claimants face to face e.g. Jobcentres, and the CHRA will be completed by sites that deal with claimants by telephone e.g. legacy sites and pensions, refer to the Contact Centre H&S Framework for a definition of what constitutes a contact centre.

11.2 At the initial review the Site Manager will:

11.2.1 Meet the TU Appointed Safety Representative (if they wish to attend);

11.2.2 Consider any comments;

11.2.3 Take the last CHRA or JCFRA to review;

11.2.4 Examine relevant documentation gathered;

11.2.5 Conduct an examination of the claimant facing area (if necessary);

11.2.6 Ensure that all existing control measures recorded on the CHRA and JCFRA are in place and are being followed;

11.2.7 Consider any new evidence and impact it against the CHRA and JCFRA (especially the activities/controls affected by any significant change (e.g. new work practices, office layout changes or a fast track incident));

11.2.8 Decide whether those control measures recorded on the CHRA and JCFRA are suitable and sufficient or whether additional control measures should be considered.

11.3 Where the review indicates that the CHRA and JCFRA remains suitable and sufficient to manage the risks then no changes to it will be required. This will be the case for the majority of annual reviews provided the CHRA and JCFRA have been reviewed on an on-going basis to address significant changes as they occur.

11.4 Where the review indicates that the CHRA and JCFRA may be no longer suitable and sufficient to manage the risks (e.g. as a result of significant changes to new work practices, office layout changes or a fast track incident) then a further review (and if necessary revision) must be carried out by the Site Manager in partnership with the Risk Assessor.

11.5 If there is any doubt regarding the suitability of control measures that are the Security Services Provider responsibility to implement (e.g. numbers of CCO's, CCTV systems, digilocks etc.) then a review of the Security Risk Assessment should be ordered via the Integrator helpdesk

11.6 Site Managers should consult with the Trade Union Appointed Safety Representative about arranging the further review and gather all necessary documentation to enable it to take place following the guidance arranging the review of the CHRA and JCFRA

11.7 The completed CFRA and JCFRA must be stored in a separate folder on the IT system. The date of the assessment and name of the office must be included in the file name. A separate file must be kept for every review for audit purposes and these should be retained for a minimum of 6 years.

11.8 All reviews (and if necessary further reviews and revisions) must be signed off at the relevant section of the CHRA and JCFRA.

12 Action to Take Where Agreement Cannot be Reached

12.1 Exceptionally, the Site Manager and the Risk Assessor may feel unable to agree about all of the recommendations made. Areas of concern should be discussed in detail with the Risk Assessor and a record of the outcome retained with the report. Any relevant additional information that was not available during the CHRA and JCFRA (or review) may be taken into account.

12.2 If issues still remain, the Site Manager should consult the Senior Manager in an attempt to resolve them.

12.3 There may be occasions where the TU Appointed Safety Representative states that they are not content with the CHRA and JCFRA (or review) findings. The Site Manager should request that TU set out their concerns in writing, normally within 10 working days. The Site Manager may wish to consult the Senior Manager, HSBP and/or the Risk Assessor before responding in writing, following further consideration. A record of these discussions should be retained with the CHRA and JCFRA.

12.4 The final decision on the implementation of control measures in all cases where agreement cannot be reached will ultimately rest with the Senior Manager.

13 Complaints about Service Provision

13.1 If the Site Manager is not satisfied with the service provided, action should be taken as outlined in Health & Safety Provision.

Annex 1 – Claimant Handling Risk Assessment Prompt Sheet

[REDACTED]

Useful links

JCFRA Guidance

Call Handlers Health & Safety Checklist

Environment

Incident Management Plan

Incidents

Accidents

Designing Out Risk in Policy Development

Staff Protection List

Managing Freedom and Flexibilities within the Jobcentre Plus Environment Guide (JPEG)

JPEG

First Aid

DSE Training and Workstation RA

Eye Care

Annex 2 – Claimant Handling Risk Assessment Blank Form

[REDACTED]

Annex 3 – Call Handling Risk Assessment Example

[REDACTED]

Annex 4 – Jobcentre Claimant Facing Risk Assessment Prompt Sheet

[REDACTED]

Annex 5 – Jobcentre Claimant Facing Risk Assessment Blank Form

[REDACTED]

Annex 6 – Jobcentre Claimant Facing Risk Assessment Example

[REDACTED]

Part 18 – Not used

Part 19 – Unacceptable Customer Behaviour Policy

[REDACTED]

Part 20 – Small / Medium Enterprise Policy

Use of SMEs in the Contractor's Supply Chain

The Authority recognises the important role small and medium enterprises (SMEs) have in helping to deliver economic growth and prosperity. SMEs are defined as enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding 50 million euro, and/or an annual balance sheet total not exceeding 43 million euro. The Authority is committed to supporting the government's target of 25% of government spending with third party suppliers to go to SMEs through either direct spend or indirectly through the supply chain where it is relevant to the contractual requirement to do so and provides value for money.

Part 21 – Common Civil Service Pass Guidance

Common Civil Service Pass (CCSP)

Cabinet Office

Version History

SPF Version	Document Version	Date Published	Summary Of Changes
April 2015	N/A	August 2015	‘Protocols for the Common Civil Service Pass’ and ‘Common Civil Service Pass-FAQs’ documents consolidated and minor amendments to guidance.

Cabinet Office

Contents

Overview 4

Key Principles 4

Who is eligible for a CCSP? 5

Full access (staff) passes 5

Limited access (Contractors) passes 5

How should CCSPs be produced? 6

How are CCSPs verified? 7

What level of access does the CCSP provide across different sites? 8

How should CCSPs be managed? 9

The CCSP and clearance 9

Full access (staff) passes 9

Limited access (contractor) passes 10

Loss of passes 10

What communication should be provided to passholders? 10

Next steps – moving to an Automated Access Control System (AACS) 11

Annexes

Annex A – Departmental baseline security levels 12

Annex B – Access verification process STAFF 13

Annex C – Access verification process CONTRACTOR 14

Overview

14 The Common Civil Service Pass (CCSP) provides for uniform but not universal access to common areas of HMG buildings, supporting flexible cross- departmental working and the sharing of facilities and estates. This guidance outlines the protocols for the issuing, use and expiry of the CCSP across central government departments, agencies and their wider delivery families.

15 Any comments or questions should be directed to Government Security Secretariat (GSS) in the Cabinet Office by email: [REDACTED]

Key Principles

16 The following principles should be applied to ensure consistent approaches and manage the associated security risks:

- Full access (staff) and limited access (contractor) passes should be provided as appropriate to individuals, according to their employment status and level of security vetting.
- Possession of a CCSP should be accepted as de facto confirmation that an individual holds the relevant personnel security control (BPSS or a National Security Vetting level). See the '*Who is eligible for a CCSP?*' section for first time procedures to confirm a new pass holder's clearance level. Security clearance levels are marked by the following colours:

[REDACTED]

- The majority of government business is managed at OFFICIAL, with a baseline BPSS requirement for unescorted access to most, but not all, HMG buildings[1]. All Civil Service pass holders should be able to access the common areas of these buildings with the minimum of fuss.
- Additional assurances may be appropriate in the following cases:
  - Buildings that are assessed to be at high risk of terrorist attack, requiring CTC or above security clearance for access;
  - Designated areas, or entire buildings, where highly sensitive assets are managed, to ensure effective access control;
  - Where specific legal requirements apply to control access.
- Departments and agencies must ensure that enhanced security measures can be put in place (or removed) at short notice in response to any change in the HMG Response Level.
- Changes to the HMG estate and increasing use of flexible working means that staff are increasingly working across multiple sites. CCSP passholders visiting another department should, as standard, be allowed to escort non-CCSP passholder visitors, provided that entry requirements for that visitor are met. Escorting rights may be reduced according to local security requirements, however, any restriction on escorting permissions must be clearly justified. Where permissions are unclear, they should be confirmed in advance with the relevant department.

---

[1] Details of the clearance level required for access to HMG buildings are at Annex A.

Who is eligible for a CCSP?

17 First time passes (including for individuals moving department, whether permanently or on loan) require a two-stage verification ensuring that:

1) The individual holds a job, subject to security checks, within your organisation (this can be confirmed by their new Line Manager or, in most cases, a central HR team)
2) The individual holds the level of clearance that they have declared (the process for confirming this should be agreed with Departmental Security Units)

18 Central departments and agencies are responsible for determining who gets a CCSP. However, the following would qualify.

19 **Full access (staff) passes may be issued to the following:**

- Permanent employees (including military personnel as required) ● Temporary staff (including staff on loan)
- Wider Departmental family (NDPBs, delivery partners, GoCo's etc)
- Regular visitors from other Public Sector organisations (e.g. Police, NHS, Local Government) requiring multi-departmental access – issued at the discretion of the DSO[2]
- In some circumstances where there is a genuine requirement for embedded contractors/private industry partners to work broadly across HMG – issued at the discretion of the DSO

20 **Limited access (contractors) passes** do not provide the same level of access as a full access pass. Unescorted access is limited to sponsor department locations only – either to a specific site or as determined by the department. They may be issued to the following:

- Consultants and / or industry secondees embedded in specific business units ● Contractors providing specific corporate services (e.g. FM staff, builders, cleaners and others)[3]
- Regular visitors from other Public Sector organisations (e.g. Police, NHS, Local Government) requiring access to a limited number of departments – issued at the discretion of the DSO
- Regular external visitors (non-Public Sector) – issued at the discretion of the DSO

21 In certain circumstances departments may wish to enter into bi-lateral agreements to allow limited access (contractor) pass holders from an OGD unescorted access into their buildings – this should be based on departmental requirements and front desk and guarding staff should be made fully aware of requirements.

22 For some individuals working alongside a department but not falling into any of the above categories, such as those from unrelated public or private sector organisations sharing office space, it would not be appropriate to issue a CCSP. Departments should issue such individuals with either a building or temporary visitors' pass, in order to provide local access.

---

[2] Taking into account the case for access, local risk appetite and the views of other departments affected.

[3] It may not be appropriate or necessary to provide CCSPs for these individuals, however DSUs

should decide based upon business need.

23 Bespoke arrangements may be appropriate to manage specific sensitivities, such as foreign nationals working in areas where access to sensitive information must be tightly controlled.

How should CCSPs be produced?

24 The integrity of the CCSP design is paramount. The effectiveness of the CCSP system rests on passes being recognisable and verifiable across sites and departments. The requirements set out in the *'Guidance for Production'*[4] document must be followed in all instances and any changes to these will be centrally driven and communicated. If a particular local requirement arises then departments should discuss this with GSS.

25 Only valid departmental codes, agreed with GSS[5], should be printed on CCSPs. It is a parent department's responsibility to develop codes for their agencies and NDPBs, these should start with the parent department code and be suffixed with A; B; C etc. At multi-occupancy sites staff should be provided with a pass that bears the code of the department they are working for. Loan staff should also be provided with a pass that bears the code of the department they are working for.

26 As management of CCSPs remains at local level, the reverse side of CCSPs should be printed with the information that departments previously provided on departmental passes. Example wording is available in the 'Guidance for Production' document and should include instructions for the handling of the pass in case of one being found. It is best practice to print a coloured stripe on the back of the card, though this is not essential and not all departmental printing facilities will allow this.

How are CCSPs verified?

27 When entering a building reception staff and/or guards should check the following before allowing CCSP holders access to a building (process diagrams are provided at Annex B and C):

- Photo
- Departmental Code – for additional assurance reception staff and / or guards may verbally challenge pass holders against the official code list[6]
- Expiry date (refer to the table below for details of CCSP validity periods)
- Clearance
- Name – when visit notification is required

---

[4] Available on the CPNI Extranet or from GSS

[5] New codes should be emailed to [REDACTED]

[6] Updated periodically and available from the CPNI Extranet

28 Where appropriate, holders of a common Civil Service pass should be allowed unescorted access without needing an additional visitor pass, though a technologically enabled site pass may be issued where internal barriers are in place.

29 Where an individual's security clearance is not equivalent to building security requirements, or where a Contractor (limited access) pass is held, the front desk should be notified to expect an OGD visitor and normal access and escorting procedures will apply.

30 If there is any doubt as to the authenticity of a pass, local security policies should stipulate whether alternative forms of identification may be acceptable and thee home department DSU of the passholder should be notified.

Cabinet Office

What level of access does the CCSP provide across different sites?

[REDACTED]

- The common pass will grant access to common areas of a HMG building, however it will not grant universal access. Restricted areas, where highly sensitive assets are managed will not be accessible.

---

[7] A list of HMG departments and their baseline security levels can be found at Annex A

[8]

How should CCSPs be managed?

The CCSP and clearance

31 Eligible individuals should be issued with a pass according to their clearance level, which is determined by the requirements of the post that they hold (ie. a post may require BPSS or a NSV level). Since clearances are post specific, they will lapse after one year (six months if an individual has been working overseas and not in an overseas British diplomatic mission or similar assignment, within an EU or NATO mission) if no longer required.

32 Should a member of staff move to a post that requires lower clearance, they should be issued a new CCSP appropriate to the requirement of that post. However, in circumstances where there is a strong case for a clearance to be maintained, and at the discretion of their original vetting sponsor and DSU in their new post, an individual may retain their prior clearance level and therefore be issued with a pass that reflects this, provided that the on-going personnel security requirements for that clearance level are met.

33 Individuals employed by departments on a risk-managed basis prior to all BPSS checks being completed must not be issued with a common pass until these are complete.

Full access (staff) passes

34 An individual should never hold more than one CCSP at any one time. New joiners and staff moving departments (whether temporarily or permanently) should be issued with a CCSP for their new department, linked to that department's access control system and displaying that department's code. For instance, a Home Office employee on loan to the Cabinet Office should be provided with a pass that provides access to the building in which they work on a day-to-day basis and which shows the Cabinet Office departmental code. Loan status should not be indicated on the pass.

35 Such staff should surrender their previous common pass or any other pass to their home department's DSU for the duration of the loan (a new CCSP must not be issued until this is complete). Once their loan period is complete, staff should surrender any passes from their loan department before they are issued a new pass with the code of their home department (if they are returning) or the code of their second loan department (if they have transferred their loan onwards). A staff member's pass should always display the code for the location that they work at on a day-to-day basis.

Limited access (contractor) passes

36 Contractors (and individuals eligible for a Contractor pass) should be issued with a CCSP for the department they are working with. Before issuing, contractors should be asked whether they hold any existing CCSPs and any such passes should be returned before a new CCSP is issued. Some contractors are working at multiple locations and departments may wish to enter into bi-lateral agreements to allow contractors unescorted access into more than one department. This should be based on departmental need, with front desk and guarding staff advised accordingly. Under no circumstances should a contractor be issued with multiple versions of the common pass.

Loss of passes

37 It would not be proportionate or manageable to establish a central mechanism for reporting lost or stolen Common Civil Service passes. Departments should operate their own normal procedures to ensure passes are disabled on home department AACS, as well as ensuring passes are returned by individuals when leaving the department/organisation, including when leaving on loan.

38 Where passes are being used to access OGDs, as per the supporting protocols, guards should be inspecting passes carefully. If there is any doubt as to the card's validity or authenticity, individuals

should be directed to reception where their reason for visiting can be verified (e.g. through confirming attendance with sponsor).

39 If a particular need is identified to share with other departments details of a lost or stolen pass, details of the pass may be posted on the DSO Hub.

What communication should be provided to passholders?

40 When provided with a CCSP, staff or contractors should be briefed to understand their responsibilities when escorting and working at the home department and other government departments (OGDs), including:

- Who they can and cannot escort.
- Where they can and cannot access[9].
- Their personal responsibility to protect information – applying a clear desk policy and appropriate behaviours when using telephones, faxes and printers.
- The maximum classification of information that can be worked on at OGD locations.
- A reminder to staff that the wearing of a common pass outside of HMG buildings is strictly prohibited and can result in a breach.
- Line Managers should be briefed about their responsibility to retrieve passes from any member of staff that is leaving their department and return it to the DSU.

41 Departments and agencies may wish to ensure that visiting staff are provided with simple information about local security policies, Health and Safety requirements, and evacuation procedures for the site.

Next steps – moving to an Automated Access Control System (AACS)

Cabinet Office is working with CESG and departments to set a framework for technical standards to underpin departments' chosen card/reader/database systems. In the first instance please address any queries to [REDACTED]

[9] Annex A should be made available to staff via departmental intranet.

Cabinet Office

Annex A

Departmental baseline security levels

The table below outlines the baseline security levels for the main departmental sites in central London. You should consult this table before visiting OGDs in case you are required to provide prior notice of your visit.

[REDACTED]