OFFICE OF RAIL AND ROAD

Gleeds Cost Management Limited
95 New Cavendish Street

London

W1W 6XF

Attn: Mark Syrett

By email to: mark.syrett@gleeds.co.uk

Date: 30/08/2017

Our ref: ORR CT 17-12

Dear Sirs,

Award of contract for the supply of Specialist Contractors / Contingent Labour – Rail Enhancement Projects Cost Review

Following your tender/ proposal for the supply of specialist contractors/contingent labour to the Office of Rail and Road (**ORR**), we are pleased to award this contract to you.

This letter (Award Letter) and its Annexes set out the terms of the contract between ORR as the Customer and Gleeds Cost Management Limited as the Supplier for the provision of the Services. Unless the context otherwise requires, capitalised expressions used in this Award Letter have the same meanings as in the terms and conditions of contract set out in Annex 1 to this Award Letter (the "**Conditions**"). In the event of any conflict between this Award Letter and the Conditions, this Award Letter shall prevail. Please do not attach any Supplier terms and conditions to this Award Letter as they will not be accepted by the Customer and may delay the conclusion of the Agreement.

For the purposes of the Agreement, the Customer and the Supplier agree as follows:

1) The Services shall be performed at the Customers premises, being One Kemble Street, London, WC2B 4AN or any other location as agreed by the customer.

2) The charges for the Services shall be as set out in Annex 2.

3) The specification of the Services to be supplied is as set out in Annex 3.

4) The Term shall commence on 31/09/2017 and the Expiry Date shall be 30/09/2019.

5) The address for notices of the Parties are:

Customer

Office of Rail and Road

One Kemble Street, London, WC2B 4AN

Attention: Mayank Vyas

Email: Mayank.vyas@orr.gsi.gov.uk

Supplier

Gleeds Cost Management Limited
95 New Cavendish Street, London, W1W 6XF

Attention: Mark Syrett

Email: mark.syrett@gleeds.co.uk

6) The following persons are Key Personnel for the purposes of the Agreement:

Name and Title:

Ian Bayes – Director

Mike Beamish – Senior Consultant

Paul Carey – Director

Jeremy Evans – Managing Consultant

Richard Golding – Director

Jim Hartley – Managing Consultant

Ian Hodges – Principal Consultant

Derek Hoey – Managing Consultant

James Jenkinson – Consultant

Paul Jerrett – Senior Consultant

Martyn Jones – Senior Consultant

Glenn Lawrence – Managing Consultant

Mark Syrett – Director

Martin Smalley – Director

Richard Fluin – Director

John Gredley – Principal Consultant

Huw Kane – Director

Cara Murphy – Principal Consultant

Steve Parker – Director

Darren Self – Principal Consultant

Simon Shapiro – Managing Consultant

Anzhela Shestakova – Senior Consultant

7) For the purposes of the Agreement the data security requirements, vetting procedure and equality and diversity policy are set out in Annex 4.

8) The Customer may require the Supplier to ensure that any person employed in the provision of the Services has undertaken a Disclosure and Barring Service check. The Supplier shall ensure that no person who discloses that he/she has a conviction that is relevant to the nature of the Services, relevant to the work of the Customer, or is of a type otherwise advised by the Customer (each such conviction a "**Relevant Conviction**"), or is found by the Supplier to have a Relevant Conviction (whether as a result of a police check, a Disclosure and Barring Service check or otherwise) is employed or engaged in the provision of any part of the Services.

9) The value of the contract including any extension shall not exceed £150,000 exclusive of VAT

Payment

All invoices must be sent, quoting a valid purchase order number (PO Number), to: Accounts Payable, Office of Rail and Road, One Kemble Street, London, WC2B 4AN (accountspayable@orr.gsi.gov.uk). Within 10 working days of receipt of your countersigned copy of

this letter, we will send you a unique PO Number. You must be in receipt of a valid PO Number before submitting an invoice.

To avoid delay in payment it is important that the invoice is compliant and that it includes a valid PO Number, PO Number item number (if applicable) and the details (name and telephone number) of your Customer contact (i.e. Contract Manager). Non-compliant invoices will be sent back to you, which may lead to a delay in payment. If you have a query regarding an outstanding payment please contact our Accounts Payable section either by email to accountspayable@orr.gsi.gov.uk or by telephone 0207 282 2167 between 09:00-17:00 Monday to Friday.

Liaison

For general liaison your contact will continue to be Howard Taylor (howard.taylor@orr.gsi.gov.uk), 0207 282 2054 or, in their absence, James Dunshea (james.dunshea@orr.gsi.gov.uk) 0207 282 2064.

We thank you for your co-operation to date, and look forward to forging a successful working relationship resulting in a smooth and successful delivery of the Services. Please confirm your acceptance of the award of this contract by signing and returning the enclosed copy of this letter to Mayank Vyas via ORR's e-tendering portal **within 7** days from the date of this letter. No other form of acknowledgement will be accepted. Please remember to quote the reference number above in any future communications relating to this contract.

Yours faithfully,

Signed for and on behalf of Office of Rail and Road

Name: Mayank Vyas
Procurement and Finance Executive

Signature:

Date: 30/08/2017

We accept the terms set out in this letter and its **Annexes**, including the Conditions.

Signed for and on behalf of Gleeds Cost Management Limited

Name: MARK SYMETT
Job Title DIRECTOR.

Signature: Date: 12/9/17

12/9/17

M. B. SYMETT
DIRECTOR.

Annex 1

Terms and Conditions of Contract for Services

1 Interpretation

1.1 In these terms and conditions:

"Agreement"	means the contract between (i) the Customer acting as part of the Crown and (ii) the Supplier constituted by the Supplier's countersignature of the Award Letter and includes the Award Letter and Annexes;
"Award Letter"	means the letter from the Customer to the Supplier printed above these terms and conditions;
"Central Government Body"	means a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics: (a) Government Department; (b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal); (c) Non-Ministerial Department; or (d) Executive Agency;
"Charges"	means the charges for the Services as specified in the Award Letter;
"Confidential Information"	means all information, whether written or oral (however recorded), provided by the disclosing Party to the receiving Party and which (i) is known by the receiving Party to be confidential; (ii) is marked as or stated to be confidential; or (iii) ought reasonably to be considered by the receiving Party to be confidential;
"Customer"	means the person named as Customer in the Award Letter;
"DPA"	means the Data Protection Act 1998;
"Expiry Date"	means the date for expiry of the Agreement as set out in the Award Letter;
"FOIA"	means the Freedom of Information Act 2000;
"Information"	has the meaning given under section 84 of the FOIA;
"Key Personnel"	means any persons specified as such in the Award Letter or otherwise notified as such by the Customer to the Supplier in writing;
"Party"	means the Supplier or the Customer (as appropriate) and "Parties" shall mean both of them;
"Personal Data"	means personal data (as defined in the DPA) which is processed by the Supplier or any Staff on behalf of the Customer pursuant to or in connection with this Agreement;
"Purchase Order Number"	means the Customer's unique number relating to the supply of the Services;
"Request for Information"	has the meaning set out in the FOIA or the Environmental Information Regulations 2004 as relevant (where the meaning set

	out for the term "request" shall apply);
"Services"	means the services to be supplied by the Supplier to the Customer under the Agreement;
"Specification"	means the specification for the Services (including as to quantity, description and quality) as specified in the Award Letter;
"Staff"	means all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any sub-contractor of the Supplier engaged in the performance of the Supplier's obligations under the Agreement;
"Staff Vetting Procedures"	means vetting procedures that accord with good industry practice or, where requested by the Customer, the Customer's procedures for the vetting of personnel as provided to the Supplier from time to time;
"Supplier"	means the person named as Supplier in the Award Letter;
"Term"	means the period from the start date of the Agreement set out in the Award Letter to the Expiry Date as such period may be extended in accordance with clause 4.2 or terminated in accordance with the terms and conditions of the Agreement;
"VAT"	means value added tax in accordance with the provisions of the Value Added Tax Act 1994; and
"Working Day"	means a day (other than a Saturday or Sunday) on which banks are open for business in the City of London.

1.2 In these terms and conditions, unless the context otherwise requires:

1.2.1 references to numbered clauses are references to the relevant clause in these terms and conditions;

1.2.2 any obligation on any Party not to do or omit to do anything shall include an obligation not to allow that thing to be done or omitted to be done;

1.2.3 the headings to the clauses of these terms and conditions are for information only and do not affect the interpretation of the Agreement;

1.2.4 any reference to an enactment includes reference to that enactment as amended or replaced from time to time and to any subordinate legislation or byelaw made under that enactment; and

1.2.5 the word 'including' shall be understood as meaning 'including without limitation'.

2 Basis of Agreement

2.1 The Award Letter constitutes an offer by the Customer to purchase the Services subject to and in accordance with the terms and conditions of the Agreement.

2.2 The offer comprised in the Award Letter shall be deemed to be accepted by the Supplier on receipt by the Customer of a copy of the Award Letter countersigned by the Supplier within [7] days of the date of the Award Letter.

3 Supply of Services

3.1 In consideration of the Customer's agreement to pay the Charges, the Supplier shall supply the Services to the Customer for the Term subject to and in accordance with the terms and conditions of the Agreement.

3.2 In supplying the Services, the Supplier shall:

3.2.1 co-operate with the Customer in all matters relating to the Services and comply with all the Customer's instructions;

3.2.2 perform the Services with all reasonable care, skill and diligence in accordance with good industry practice in the Supplier's industry, profession or trade;

3.2.3 use Staff who are suitably skilled and experienced to perform tasks assigned to them, and in sufficient number to ensure that the Supplier's obligations are fulfilled in accordance with the Agreement;

3.2.4 ensure that the Services shall conform with all descriptions and specifications set out in the Specification;

3.2.5 comply with all applicable laws; and

3.2.6 provide all equipment, tools and vehicles and other items as are required to provide the Services.

3.3 The Customer may by written notice to the Supplier at any time request a variation to the scope of the Services. In the event that the Supplier agrees to any variation to the scope of the Services, the Charges shall be subject to fair and reasonable adjustment to be agreed in writing between the Customer and the Supplier.

4 Term

4.1 The Agreement shall take effect on the date specified in Award Letter and shall expire on the Expiry Date, unless it is otherwise extended in accordance with clause 4.2 or terminated in accordance with the terms and conditions of the Agreement.

4.2 The Customer may extend the Agreement for a period of up to 6 months by giving not less than 10 Working Days' notice in writing to the Supplier prior to the Expiry Date. The value of the contract including any extension shall not exceed One hundred and fifty thousand pounds [£150,000] in total. The terms and conditions of the Agreement shall apply throughout any such extended period.

5 Charges, Payment and Recovery of Sums Due

5.1 The Charges for the Services shall be as set out in the Award Letter and shall be the full and exclusive remuneration of the Supplier in respect of the supply of the Services. Unless otherwise agreed in writing by the Customer, the Charges shall include every cost and expense of the Supplier directly or indirectly incurred in connection with the performance of the Services.

5.2 All amounts stated are exclusive of VAT which shall be charged at the prevailing rate. The Customer shall, following the receipt of a valid VAT invoice, pay to the Supplier a sum equal to the VAT chargeable in respect of the Services.

5.3 The Supplier shall invoice the Customer as specified in the Agreement. Each invoice shall include such supporting information required by the Customer to verify the accuracy of the invoice, including the relevant Purchase Order Number and a breakdown of the Services supplied in the invoice period.

5.4 In consideration of the supply of the Services by the Supplier, the Customer shall pay the Supplier the invoiced amounts no later than 30 days after verifying that the invoice is valid and undisputed and includes a valid Purchase Order Number. The Customer may, without prejudice to any other rights and remedies under the Agreement, withhold or reduce payments in the event of unsatisfactory performance.

5.5 If the Customer fails to consider and verify an invoice in a timely fashion the invoice shall be regarded as valid and undisputed for the purpose of paragraph 5.4 after a reasonable time has passed.

5.6 If there is a dispute between the Parties as to the amount invoiced, the Customer shall pay the undisputed amount. The Supplier shall not suspend the supply of the Services unless the Supplier is entitled to terminate the Agreement for a failure to pay undisputed sums in accordance with clause 16.4. Any disputed amounts shall be resolved through the dispute resolution procedure detailed in clause 19.

5.7 If a payment of an undisputed amount is not made by the Customer by the due date, then the Customer shall pay the Supplier interest at the interest rate specified in the Late Payment of Commercial Debts (Interest) Act 1998.

5.8 Where the Supplier enters into a sub-contract, the Supplier shall include in that sub-contract:

5.8.1 provisions having the same effects as clauses 5.3 to 5.7 of this Agreement; and

5.8.2 a provision requiring the counterparty to that sub-contract to include in any sub-contract which it awards provisions having the same effect as 5.3 to 5.8 of this Agreement.

5.8.3 In this clause 5.8, "sub-contract" means a contract between two or more suppliers, at any stage of remoteness from the Authority in a subcontracting chain, made wholly or substantially for the purpose of performing (or contributing to the performance of) the whole or any part of this Agreement.

5.9 If any sum of money is recoverable from or payable by the Supplier under the Agreement (including any sum which the Supplier is liable to pay to the Customer in respect of any breach of the Agreement), that sum may be deducted unilaterally by the Customer from any sum then due, or which may come due, to the Supplier under the Agreement or under any other agreement or contract with the Customer. The Supplier shall not be entitled to assert any credit, set-off or counterclaim against the Customer in order to justify withholding payment of any such amount in whole or in part.

6 Premises and equipment

6.1 If necessary, the Customer shall provide the Supplier with reasonable access at reasonable times to its premises for the purpose of supplying the Services. All equipment, tools and vehicles brought onto the Customer's premises by the Supplier or the Staff shall be at the Supplier's risk.

6.2 If the Supplier supplies all or any of the Services at or from the Customer's premises, on completion of the Services or termination or expiry of the Agreement (whichever is the earlier) the Supplier shall vacate the Customer's premises, remove the Supplier's plant, equipment and unused materials and all rubbish arising out of the provision of the Services and leave the Customer's premises in a clean, safe and tidy condition. The Supplier shall be solely responsible for making good any damage to the Customer's premises or any objects contained on the Customer's premises which is caused by the Supplier or any Staff, other than fair wear and tear.

6.3 If the Supplier supplies all or any of the Services at or from its premises or the premises of a third party, the Customer may, during normal business hours and on reasonable notice, inspect and examine the manner in which the relevant Services are supplied at or from the relevant premises.

6.4 The Customer shall be responsible for maintaining the security of its premises in accordance with its standard security requirements. While on the Customer's premises the Supplier shall, and shall procure that all Staff shall, comply with all the Customer's security requirements.

6.5 Where all or any of the Services are supplied from the Supplier's premises, the Supplier shall, at its own cost, comply with all security requirements specified by the Customer in writing.

6.6 Without prejudice to clause 3.2.6, any equipment provided by the Customer for the purposes of the Agreement shall remain the property of the Customer and shall be used by the Supplier and the Staff only for the purpose of carrying out the Agreement. Such equipment shall be returned promptly to the Customer on expiry or termination of the Agreement.

6.7 The Supplier shall reimburse the Customer for any loss or damage to the equipment (other than deterioration resulting from normal and proper use) caused by the Supplier or any Staff. Equipment supplied by the Customer shall be deemed to be in a good condition when received by the Supplier or relevant Staff unless the Customer is notified otherwise in writing within 5 Working Days.

7 Staff and Key Personnel

7.1 If the Customer reasonably believes that any of the Staff are unsuitable to undertake work in respect of the Agreement, it may, by giving written notice to the Supplier:

7.1.1 refuse admission to the relevant person(s) to the Customer's premises;

7.1.2 direct the Supplier to end the involvement in the provision of the Services of the relevant person(s); and/or

7.1.3 require that the Supplier replace any person removed under this clause with another suitably qualified person and procure that any security pass issued by the Customer to the person removed is surrendered,

and the Supplier shall comply with any such notice.

7.2 The Supplier shall:

7.2.1 ensure that all Staff are vetted in accordance with the Staff Vetting Procedures;

7.2.2 if requested, provide the Customer with a list of the names and addresses (and any other relevant information) of all persons who may require admission to the Customer's premises in connection with the Agreement; and

7.2.3 procure that all Staff comply with any rules, regulations and requirements reasonably specified by the Customer.

7.3 Any Key Personnel shall not be released from supplying the Services without the agreement of the Customer, except by reason of long-term sickness, maternity leave, paternity leave, termination of employment or other extenuating circumstances.

7.4 Any replacements to the Key Personnel shall be subject to the prior written agreement of the Customer (not to be unreasonably withheld). Such replacements shall be of at least equal status or of equivalent experience and skills to the Key Personnel being replaced and be suitable for the responsibilities of that person in relation to the Services.

8 Assignment and sub-contracting

8.1 The Supplier shall not without the written consent of the Customer assign, sub-contract, novate or in any way dispose of the benefit and/ or the burden of the Agreement or any part of the Agreement. The Customer may, in the granting of such consent, provide for additional terms and conditions relating to such assignment, sub-contract, novation or disposal. The Supplier shall be responsible for the acts and omissions of its sub-contractors as though those acts and omissions were its own.

8.2 Where the Customer has consented to the placing of sub-contracts, the Supplier shall, at the request of the Customer, send copies of each sub-contract, to the Customer as soon as is reasonably practicable.

8.3 The Customer may assign, novate, or otherwise dispose of its rights and obligations under the Agreement without the consent of the Supplier provided that such assignment, novation or disposal shall not increase the burden of the Supplier's obligations under the Agreement.

9 Intellectual Property Rights

9.1 All intellectual property rights in any materials provided by the Customer to the Supplier for the purposes of this Agreement shall remain the property of the Customer but the Customer hereby grants the Supplier a royalty-free, non-exclusive and non-transferable licence to use such materials as required until termination or expiry of the Agreement for the sole purpose of enabling the Supplier to perform its obligations under the Agreement.

9.2 All intellectual property rights in any materials created or developed by the Supplier pursuant to the Agreement or arising as a result of the provision of the Services shall vest in the Supplier. If, and to the extent, that any intellectual property rights in such materials vest in the Customer by operation of law, the Customer hereby assigns to the Supplier by way of a present assignment of future rights that shall take place immediately on the coming into existence of any such intellectual property rights all its intellectual property rights in such materials (with full title guarantee and free from all third party rights).

9.3 The Supplier hereby grants the Customer:

9.3.1 a perpetual, royalty-free, irrevocable, non-exclusive licence (with a right to sub-license) to use all intellectual property rights in the materials created or developed pursuant to the Agreement and any intellectual property rights arising as a result of the provision of the Services; and

9.3.2 a perpetual, royalty-free, irrevocable and non-exclusive licence (with a right to sub-license) to use:

(a) any intellectual property rights vested in or licensed to the Supplier on the date of the Agreement; and

(b) any intellectual property rights created during the Term but which are neither created or developed pursuant to the Agreement nor arise as a result of the provision of the Services,

including any modifications to or derivative versions of any such intellectual property rights, which the Customer reasonably requires in order to exercise its rights and take the benefit of the Agreement including the Services provided.

9.4 The Supplier shall indemnify, and keep indemnified, the Customer in full against all costs, expenses, damages and losses (whether direct or indirect), including any interest, penalties, and reasonable legal and other professional fees awarded

against or incurred or paid by the Customer as a result of or in connection with any claim made against the Customer for actual or alleged infringement of a third party's intellectual property arising out of, or in connection with, the supply or use of the Services, to the extent that the claim is attributable to the acts or omission of the Supplier or any Staff.

10 Governance and Records

10.1 The Supplier shall:

10.1.1 attend progress meetings with the Customer at the frequency and times specified by the Customer and shall ensure that its representatives are suitably qualified to attend such meetings; and

10.1.2 submit progress reports to the Customer at the times and in the format specified by the Customer.

10.2 The Supplier shall keep and maintain until 6 years after the end of the Agreement, or as long a period as may be agreed between the Parties, full and accurate records of the Agreement including the Services supplied under it and all payments made by the Customer. The Supplier shall on request afford the Customer or the Customer's representatives such access to those records as may be reasonably requested by the Customer in connection with the Agreement.

11 Confidentiality, Transparency and Publicity

11.1 Subject to clause 11.2, each Party shall:

11.1.1 treat all Confidential Information it receives as confidential, safeguard it accordingly and not disclose it to any other person without the prior written permission of the disclosing Party; and

11.1.2 not use or exploit the disclosing Party's Confidential Information in any way except for the purposes anticipated under the Agreement.

11.2 Notwithstanding clause 11.1, a Party may disclose Confidential Information which it receives from the other Party:

11.2.1 where disclosure is required by applicable law or by a court of competent jurisdiction;

11.2.2 to its auditors or for the purposes of regulatory requirements;

11.2.3 on a confidential basis, to its professional advisers;

11.2.4 to the Serious Fraud Office where the Party has reasonable grounds to believe that the other Party is involved in activity that may constitute a criminal offence under the Bribery Act 2010;

11.2.5 where the receiving Party is the Supplier, to the Staff on a need to know basis to enable performance of the Supplier's obligations under the Agreement provided that the Supplier shall procure that any Staff to whom it discloses Confidential Information pursuant to this clause 11.2.5 shall observe the Supplier's confidentiality obligations under the Agreement; and

11.2.6 where the receiving Party is the Customer:

(a) on a confidential basis to the employees, agents, consultants and contractors of the Customer;

(b) on a confidential basis to any other Central Government Body, any successor body to a Central Government Body or any company to

which the Customer transfers or proposes to transfer all or any part of its business;

(c) to the extent that the Customer (acting reasonably) deems disclosure necessary or appropriate in the course of carrying out its public functions; or

(d) in accordance with clause 12.

and for the purposes of the foregoing, references to disclosure on a confidential basis shall mean disclosure subject to a confidentiality agreement or arrangement containing terms no less stringent than those placed on the Customer under this clause 11.

11.3 The Parties acknowledge that, except for any information which is exempt from disclosure in accordance with the provisions of the FOIA, the content of the Agreement is not Confidential Information and the Supplier hereby gives its consent for the Customer to publish this Agreement in its entirety to the general public (but with any information that is exempt from disclosure in accordance with the FOIA redacted) including any changes to the Agreement agreed from time to time. The Customer may consult with the Supplier to inform its decision regarding any redactions but shall have the final decision in its absolute discretion whether any of the content of the Agreement is exempt from disclosure in accordance with the provisions of the FOIA.

11.4 The Supplier shall not, and shall take reasonable steps to ensure that the Staff shall not, make any press announcement or publicise the Agreement or any part of the Agreement in any way, except with the prior written consent of the Customer.

12 Freedom of Information

12.1 The Supplier acknowledges that the Customer is subject to the requirements of the FOIA and the Environmental Information Regulations 2004 and shall:

12.1.1 provide all necessary assistance and cooperation as reasonably requested by the Customer to enable the Customer to comply with its obligations under the FOIA and the Environmental Information Regulations 2004;

12.1.2 transfer to the Customer all Requests for Information relating to this Agreement that it receives as soon as practicable and in any event within 2 Working Days of receipt;

12.1.3 provide the Customer with a copy of all Information belonging to the Customer requested in the Request for Information which is in its possession or control in the form that the Customer requires within 5 Working Days (or such other period as the Customer may reasonably specify) of the Customer's request for such Information; and

12.1.4 not respond directly to a Request for Information unless authorised in writing to do so by the Customer.

12.2 The Supplier acknowledges that the Customer may be required under the FOIA and the Environmental Information Regulations 2004 to disclose Information concerning the Supplier or the Services (including commercially sensitive information) without consulting or obtaining consent from the Supplier. In these circumstances the Customer shall, in accordance with any relevant guidance issued under the FOIA, take reasonable steps, where appropriate, to give the

Supplier advance notice, or failing that, to draw the disclosure to the Supplier's attention after any such disclosure.

12.3 Notwithstanding any other provision in the Agreement, the Customer shall be responsible for determining in its absolute discretion whether any Information relating to the Supplier or the Services is exempt from disclosure in accordance with the FOIA and/or the Environmental Information Regulations 2004.

13 Protection of Personal Data and Security of Data

13.1 The Supplier shall, and shall procure that all Staff shall, comply with any notification requirements under the DPA and both Parties shall duly observe all their obligations under the DPA which arise in connection with the Agreement.

13.2 Notwithstanding the general obligation in clause 13.1, where the Supplier is processing Personal Data for the Customer as a data processor (as defined by the DPA) the Supplier shall:

13.2.1 ensure that it has in place appropriate technical and organisational measures to ensure the security of the Personal Data (and to guard against unauthorised or unlawful processing of the Personal Data and against accidental loss or destruction of, or damage to, the Personal Data), as required under the Seventh Data Protection Principle in Schedule 1 to the DPA;

13.2.2 provide the Customer with such information as the Customer may reasonably request to satisfy itself that the Supplier is complying with its obligations under the DPA;

13.2.3 promptly notify the Customer of:

(a) any breach of the security requirements of the Customer as referred to in clause 13.3; and
(b) any request for personal data; and

13.2.4 ensure that it does not knowingly or negligently do or omit to do anything which places the Customer in breach of the Customer's obligations under the DPA.

13.3 When handling Customer data (whether or not Personal Data), the Supplier shall ensure the security of the data is maintained in line with the security requirements of the Customer as notified to the Supplier from time to time.

14 Liability

14.1 The Supplier shall not be responsible for any injury, loss, damage, cost or expense suffered by the Customer if and to the extent that it is caused by the negligence or wilful misconduct of the Customer or by breach by the Customer of its obligations under the Agreement.

14.2 Subject always to clauses 14.3 and 14.4:

14.2.1 the aggregate liability of the Supplier in respect of all defaults, claims, losses or damages howsoever caused, whether arising from breach of the Agreement, the supply or failure to supply of the Services, misrepresentation (whether tortuous or statutory), tort (including negligence), breach of statutory duty or otherwise shall in no event exceed a sum equal to 125% of the Charges paid or payable to the Supplier; and

14.2.2 except in the case of claims arising under clauses 9.4 and 18.3, in no event shall the Supplier be liable to the Customer for any:

(a) loss of profits;

(b) loss of business;

(c) loss of revenue;

(d) loss of or damage to goodwill;

(e) loss of savings (whether anticipated or otherwise); and/or

(f) any indirect, special or consequential loss or damage.

14.3 Nothing in the Agreement shall be construed to limit or exclude either Party's liability for:

14.3.1 death or personal injury caused by its negligence or that of its Staff;

14.3.2 fraud or fraudulent misrepresentation by it or that of its Staff; or

14.3.3 any other matter which, by law, may not be excluded or limited.

14.4 The Supplier's liability under the indemnity in clause 9.4 and 18.3 shall be unlimited.

15 Force Majeure

Neither Party shall have any liability under or be deemed to be in breach of the Agreement for any delays or failures in performance of the Agreement which result from circumstances beyond the reasonable control of the Party affected. Each Party shall promptly notify the other Party in writing when such circumstances cause a delay or failure in performance and when they cease to do so. If such circumstances continue for a continuous period of more than two months, either Party may terminate the Agreement by written notice to the other Party.

16 Termination

16.1 The Customer may terminate the Agreement at any time by notice in writing to the Supplier to take effect on any date falling at least 1 month (or, if the Agreement is less than 3 months in duration, at least 10 Working Days) later than the date of service of the relevant notice.

16.2 Without prejudice to any other right or remedy it might have, the Customer may terminate the Agreement by written notice to the Supplier with immediate effect if the Supplier:

16.2.1 (without prejudice to clause 16.2.5), is in material breach of any obligation under the Agreement which is not capable of remedy;

16.2.2 repeatedly breaches any of the terms and conditions of the Agreement in such a manner as to reasonably justify the opinion that its conduct is inconsistent with it having the intention or ability to give effect to the terms and conditions of the Agreement;

16.2.3 is in material breach of any obligation which is capable of remedy, and that breach is not remedied within 30 days of the Supplier receiving notice specifying the breach and requiring it to be remedied;

16.2.4 undergoes a change of control within the meaning of section 416 of the Income and Corporation Taxes Act 1988;

16.2.5 breaches any of the provisions of clauses 7.2, 11, 12, 13 and 17;

16.2.6 becomes insolvent, or if an order is made or a resolution is passed for the winding up of the Supplier (other than voluntarily for the purpose of solvent amalgamation or reconstruction), or if an administrator or administrative receiver is appointed in respect of the whole or any part of the Supplier's assets or business, or if the Supplier makes any

composition with its creditors or takes or suffers any similar or analogous action (to any of the actions detailed in this clause 16.2.6) in consequence of debt in any jurisdiction; or

16.2.7 fails to comply with legal obligations in the fields of environmental, social or labour law.

16.3 The Supplier shall notify the Customer as soon as practicable of any change of control as referred to in clause 16.2.4 or any potential such change of control.

16.4 The Supplier may terminate the Agreement by written notice to the Customer if the Customer has not paid any undisputed amounts within 90 days of them falling due.

16.5 Termination or expiry of the Agreement shall be without prejudice to the rights of either Party accrued prior to termination or expiry and shall not affect the continuing rights of the Parties under this clause and clauses 2, 3.2, 6.1, 6.2, 6.6, 6.7, 7, 9, 10.2, 11, 12, 13, 14, 16.6, 17.4, 18.3, 19 and 20.7 or any other provision of the Agreement that either expressly or by implication has effect after termination.

16.6 Upon termination or expiry of the Agreement, the Supplier shall:

16.6.1 give all reasonable assistance to the Customer and any incoming supplier of the Services; and

16.6.2 return all requested documents, information and data to the Customer as soon as reasonably practicable.

17 Compliance

17.1 The Supplier shall promptly notify the Customer of any health and safety hazards which may arise in connection with the performance of its obligations under the Agreement. The Customer shall promptly notify the Supplier of any health and safety hazards which may exist or arise at the Customer's premises and which may affect the Supplier in the performance of its obligations under the Agreement.

17.2 The Supplier shall:

17.2.1 comply with all the Customer's health and safety measures while on the Customer's premises; and

17.2.2 notify the Customer immediately in the event of any incident occurring in the performance of its obligations under the Agreement on the Customer's premises where that incident causes any personal injury or damage to property which could give rise to personal injury.

17.3 The Supplier shall:

17.3.1 perform its obligations under the Agreement in accordance with all applicable equality Law and the Customer's equality and diversity policy as provided to the Supplier from time to time; and

17.3.2 take all reasonable steps to secure the observance of clause 17.3.1 by all Staff.

17.4 The Supplier shall supply the Services in accordance with the Customer's environmental policy as provided to the Supplier from time to time.

17.5 The Supplier shall comply with, and shall ensure that its Staff shall comply with, the provisions of:

17.5.1 the Official Secrets Acts 1911 to 1989; and

17.5.2 section 182 of the Finance Act 1989.

18 Prevention of Fraud and Corruption

18.1 The Supplier shall not offer, give, or agree to give anything, to any person an inducement or reward for doing, refraining from doing, or for having done or refrained from doing, any act in relation to the obtaining or execution of the Agreement or for showing or refraining from showing favour or disfavour to any person in relation to the Agreement.

18.2 The Supplier shall take all reasonable steps, in accordance with good industry practice, to prevent fraud by the Staff and the Supplier (including its shareholders, members and directors) in connection with the Agreement and shall notify the Customer immediately if it has reason to suspect that any fraud has occurred or is occurring or is likely to occur.

18.3 If the Supplier or the Staff engages in conduct prohibited by clause 18.1 or commits fraud in relation to the Agreement or any other contract with the Crown (including the Customer) the Customer may:

18.3.1 terminate the Agreement and recover from the Supplier the amount of any loss suffered by the Customer resulting from the termination, including the cost reasonably incurred by the Customer of making other arrangements for the supply of the Services and any additional expenditure incurred by the Customer throughout the remainder of the Agreement; or

18.3.2 recover in full from the Supplier any other loss sustained by the Customer in consequence of any breach of this clause.

19 Dispute Resolution

19.1 The Parties shall attempt in good faith to negotiate a settlement to any dispute between them arising out of or in connection with the Agreement and such efforts shall involve the escalation of the dispute to an appropriately senior representative of each Party.

19.2 If the dispute cannot be resolved by the Parties within one month of being escalated as referred to in clause 19.1, the dispute may by agreement between the Parties be referred to a neutral adviser or mediator (the "**Mediator**") chosen by agreement between the Parties. All negotiations connected with the dispute shall be conducted in confidence and without prejudice to the rights of the Parties in any further proceedings.

19.3 If the Parties fail to appoint a Mediator within one month, or fail to enter into a written agreement resolving the dispute within one month of the Mediator being appointed, either Party may exercise any remedy it has under applicable law.

20 General

20.1 Each of the Parties represents and warrants to the other that it has full capacity and authority, and all necessary consents, licences and permissions to enter into and perform its obligations under the Agreement, and that the Agreement is executed by its duly authorised representative.

20.2 A person who is not a party to the Agreement shall have no right to enforce any of its provisions which, expressly or by implication, confer a benefit on him, without the prior written agreement of the Parties.

20.3 The Agreement cannot be varied except in writing signed by a duly authorised representative of both the Parties.

20.4 The Agreement contains the whole agreement between the Parties and

supersedes and replaces any prior written or oral agreements, representations or understandings between them. The Parties confirm that they have not entered into the Agreement on the basis of any representation that is not expressly incorporated into the Agreement. Nothing in this clause shall exclude liability for fraud or fraudulent misrepresentation.

20.5 Any waiver or relaxation either partly, or wholly of any of the terms and conditions of the Agreement shall be valid only if it is communicated to the other Party in writing and expressly stated to be a waiver. A waiver of any right or remedy arising from a breach of contract shall not constitute a waiver of any right or remedy arising from any other breach of the Agreement.

20.6 The Agreement shall not constitute or imply any partnership, joint venture, agency, fiduciary relationship or other relationship between the Parties other than the contractual relationship expressly provided for in the Agreement. Neither Party shall have, nor represent that it has, any authority to make any commitments on the other Party's behalf.

20.7 Except as otherwise expressly provided by the Agreement, all remedies available to either Party for breach of the Agreement (whether under the Agreement, statute or common law) are cumulative and may be exercised concurrently or separately, and the exercise of one remedy shall not be deemed an election of such remedy to the exclusion of other remedies.

20.8 If any provision of the Agreement is prohibited by law or judged by a court to be unlawful, void or unenforceable, the provision shall, to the extent required, be severed from the Agreement and rendered ineffective as far as possible without modifying the remaining provisions of the Agreement, and shall not in any way affect any other circumstances of or the validity or enforcement of the Agreement.

21 Notices

21.1 Any notice to be given under the Agreement shall be in writing and may be served by personal delivery, first class recorded or, subject to clause 21.3, e-mail to the address of the relevant Party set out in the Award Letter, or such other address as that Party may from time to time notify to the other Party in accordance with this clause:

21.2 Notices served as above shall be deemed served on the Working Day of delivery provided delivery is before 5.00pm on a Working Day. Otherwise delivery shall be deemed to occur on the next Working Day. An email shall be deemed delivered when sent unless an error message is received.

21.3 Notices under clauses 15 (Force Majeure) and 16 (Termination) may be served by email only if the original notice is then sent to the recipient by personal delivery or recorded delivery in the manner set out in clause 21.1.

22 Governing Law and Jurisdiction

The validity, construction and performance of the Agreement, and all contractual and non contractual matters arising out of it, shall be governed by English law and shall be subject to the exclusive jurisdiction of the English courts to which the Parties submit.

Annex 2

Charges

Name	Framework Grade	London day rate (£) Excl VAT	Glasgow day rate (£) Excl. VAT
Gleeds			
Ian Bayes	Director	937	1087
Mike Beamish	Senior Consultant	722	722
Paul Carey	Director	937	1087
Jeremy Evans	Managing Consultant	916	916
Richard Golding	Director	937	1087
Jim Hartley	Managing Consultant	766	916
Ian Hodges	Principle Consultant	700	850
Derek Hoey	Managing Consultant	766	916
James Jenkinson	Consultant	616	616
Paul Jerrett	Senior Consultant	572	722
Martyn Jones	Senior Consultant	722	722
Glenn Lawrence	Managing Consultant	722	722
Mark Syrett	Director	937	1087
Martin Smalley	Director	937	1087
GHD			
Richard Fluin	Director	937	1087
John Gredley	Principle Consultant	850	916
Huw Kane	Director	937	1087
Cara Murphy	Principle Consultant	850	916
Steve Parker	Director	937	1087
Darren Self	Principle Consultant	850	916
Simon Shapiro	Managing Consultant	850	916
Anzhela Shestakova	Senior Consultant	760	850

Annex 3

Specification

As ORR may not have sufficient internal resource (staff) to accommodate spikes in the volume of efficiency reviews required, it is looking to appoint specialist contractors to work alongside ORR's review team members in reviewing and assessing infrastructure manager's enhancement projects cost estimates to determine cost efficiency. The scope of work is for the provision of suitably qualified and experienced people (specialist contractors) to support ORR for the period of this contract.
The specialist contractor(s) will act as one of several project cost reviewers operating within the ORR team. The cost reviewer will undertake project reviews as directed by ORR using its own established methodology described below and completing the necessary paperwork in line with ORR guidelines. The specialist contractor(s) will provide advice in relation to efficient cost planning. ORR will take the final decision on any determinations or adjustments to be made through challenge and discussion of the specialist contractor(s) conclusions. The projects to be reviewed will be dependent on what is submitted to us by the infrastructure managers, our identification of poor performance, or any requests made to the ORR by funders.
The ORR envisages that the cost efficiency reviews will be on an ad-hoc basis, and may be required at short notice. The various types of cost efficiency reviews will require the same skill set, as described below.

Methodology
We have defined an internal review methodology that sets out how we review, clarify and determine efficient costs for these projects.
The ORR process for a low to medium value project is summarised below:

- ORR receives and reviews project submission pack – this takes approx. 2-3 days per project concluding with ORR submitting a question log to NR
- Workshop held with NR for them to answer questions raised in question log. NR then submit any further information required.
- Post workshop review and discussion internally – approx. 3-4 days per project
- ORR issue decision letter

For high value/complex projects or programmes a more detailed review is undertaken including pre-meetings and an extended timeframe.

For each project, the cost reviewer will fill in a template workbook (a checklist against all criteria, summary comments) which should achieve a consistent review output amongst the team and act as record of the review.

The reviewer will consider the following criteria in the review:

- Cost - Cost estimate breakdown at summary and detail level with some degree of efficiency cross-check, e.g. identified efficiencies highlighted and taken into account in the anticipated final cost (AFC), comparison with similar completed projects, direct cost proportions, unit cost analysis, justification of risk provision and uplifts, comparison to benchmarks.
- Output - the output is consistent with the funder's output statements (e.g. capacity models, or where not applicable a check against funder's business case assumptions)
- Scope - scope delivers the output; the selected option is justified on whole life cost basis, and engagement of operator has increased confidence that the solution is efficient
- Schedule/output - a delivery plan change control submission showing project milestones consistent with planned timetable changes, rolling stock / franchising plans
- VFM – evidence (letter from funder) that the cost estimate and outputs still support the business case,
- Authorisations - Defined strategy on compliance with Interoperability TSI's and other relevant statutory provisions, e.g. Project authorisation Strategy, suitably endorsed by NR's internal approval body

The ORR process for dispute resolution comprises the following key stages:

- ORR receives a formal request for resolution from the infrastructure manager or funder. Documentation is then submitted within 5 days;
- Evaluation lasts approximately 10 days, but may be extended for claims over £50m;
- ORR submits a determination and hold consultations (2 days);
- Review (3 days) and issue of a final determination.

Annex 4
ORR Policies

(a) **INTRODUC**
TION

(b) **P**
urpose

1. The purpose of this policy is to:

(a) outline the Office of Rail Regulation's (ORR) approach to equality and diversity; and

(b) summarise the rights and responsibilities of those identified within the scope of this policy.

2. This policy has been developed in consultation with Staff Side and replaces the Equal Opportunities Policy issued in 2000.

3. The policy supports the ORR's race equality scheme, which sets out how ORR will exercise its duties under the Race Relations (Amendment) Act 2000, to eliminate racial discrimination and promote equal opportunities, and how ORR intends to implement those duties day to day.

(c) **S**
cope

4. This policy provides a framework for providing a fair and equal working environment at ORR. It applies to all permanent, fixed-term and casual employees at all grades of staff throughout ORR.

5. ORR also requires all customers and third parties to abide by the ethos and guidance of this policy, including agency staff, contractors and other third parties involved in ORR's activities.

(d) **6. Employees must be aware that in some circumstances a breach of this policy may lead to disciplinary proceedings under the Discipline Policy, and**

this could lead to an employee's dismissal.

(e) **Policy statement**

7. ORR is committed to promoting an environment of equality and diversity that is free from harassment, bullying, victimisation and unfair discrimination.

8. Diversity is the concept that people should be valued as individuals and supported to maximise their potential. Diversity is not confined to ensuring that ORR complies with legislation. It creates an environment and culture where employees, third parties and customers are able to maximise their potential and, ultimately, improve the performance of the business.

9. ORR recognises and supports the business, moral and social benefits gained by supporting the principles of equality and diversity. ORR will operate these principles in employment, recruitment and selection, training, our services to customers and all other activities undertaken in our day-to-day business.

10. We will not tolerate behaviour from employees, customers or third parties engaged in our business that undermines our commitment to equality and diversity. We will take the appropriate action to prevent and correct any such actions.

11. We understand the differences between equal opportunities and diversity but believe that they are complimentary approaches to ensuring fairness in the operation of our business.

12. ORR will not unlawfully discriminate nor tolerate any discrimination from its employees, contractors or other third parties in respect of gender, marital status, race, disability, sexual orientation, transgender, religion, ethnic or national origin, caring responsibilities, trade union activities, age or any other irrelevant factor.

(f) **Respon sibility**

Employees

13. All employees referred to within the scope of this policy are required to adhere

to its terms and conditions. Employees should put the policy into practice in their day-to-day work, ensuring that they are not behaving in a way that could, intentionally or not, discriminate against others, or cause feelings of harassment, bullying or victimisation in others. Discrimination is a serious matter and the consequences of such behaviour can lead to disciplinary proceedings and also individual legal liability under the relevant legislation (see Annex A).

14. Employees must read and understand this policy, and understand that it is incorporated into their contract of employment.

Line Managers

15. Line managers are responsible for ensuring that this policy is applied within their own area. They are also responsible for creating and maintaining an environment of equality and diversity within their teams.

The Board/ Chief Executive responsibilities

16. The Board has overall responsibility for overseeing this policy and ensuring that the equality and diversity action plan is put into practice. The Chief Executive, working with the Head of HR, will ensure that all allegations of discrimination are investigated promptly and effectively, and report to the Board accordingly. The Chief Executive, working with the Head of HR, will promote an environment of equality and diversity in ORR activities.

HR

17. The Head of HR will be responsible for ensuring that the commitment to equality and diversity, as set out in this policy, underpins all aspects of HR's work.

18. All members of the HR team will be responsible for providing support and advice to employees on the application of this policy in ORR.

(g) **Duty of care**

19. ORR has a duty of care to its employees to create and maintain an environment that protects their physical and emotional well-being. We will ensure that employees do not have to work in unsafe or unhealthy conditions. This includes

protection against discrimination, harassment or bullying. An implied duty of care exists between employees and employers within all contracts of employment.

(h) **EQU**
ALITY

(i) **Equal Opportunities**
Legislation

20. ORR is committed to ensuring that it complies with all UK and European Union anti-discriminatory employment legislation. A list of relevant pieces of legislation can be found at Annex A.

(j) **Equ**
al Pay

21. ORR is committed to providing equal pay for all. Furthermore it is committed to demonstrating equal pay best practice by:

(a) having a clear and transparent pay system that has guaranteed progression through the payscales and a non-discretionary performance bonus arrangement;

(b) monitoring and reviewing the equal pay position at each pay settlement date to ensure that equal pay best practice continues to apply;

(c) ensuring quality assurance is carried out on performance box markings to ensure that there is no discrimination or bias;

(d) offering access to all pay benefits to everyone; and

(e) providing career development opportunities at all levels in the office to ensure that everyone has an equal opportunity to reach their potential.

(k) **Discrimi**
nation

22. There are two types of discrimination – direct and indirect discrimination – and in order to claim discrimination there must be UK or European Union legislation protecting the individual from such discrimination.

Direct discrimination

23. Direct discrimination occurs when a person is treated less favourably than others in the same circumstances, for example because of their:

- race, ethnic origin, nationality or skin colour;
- gender, marital status, sexual orientation, or someone who is about to undergo, or is undergoing, gender re-assignment;
- religious belief;
- disability; or
- age.

Indirect discrimination

24. Indirect discrimination is not always as obvious as direct discrimination. It occurs when a condition or requirement of employment is applied which adversely affects one particular group more than another and cannot be justified objectively by the requirements of the job, for example:

(a) unjustified selection criteria for recruitment where the proportion of, for example, one group of people who can comply is considerably lower (such as specifying that the successful candidate will have a higher education or language standard than is needed for effective performance in the job);

(b) unjustifiable requirements to work full-time. Many jobs can be adapted to accommodate part-time, job-share or flexible working arrangements; or

(c) unnecessary pressure to work in excess of conditioned hours, or an unjustifiable requirement to work early or late. This might exclude people

with domestic responsibilities from being recruited, promoted or having access to training opportunities.

Positive discrimination

25. Positive discrimination means discriminating in favour of someone from a disadvantaged group. This is generally unlawful in the UK unless there is a Genuine Occupational Qualification (GOQ), such as a female working in a women's refuge.

26. Positive action, however, involves taking steps to promote equality of opportunity in access to a post for a previously disadvantaged group. For example, providing training to allow employees from minority groups to compete on equal terms. This is legal in the UK provided that it does not guarantee a job or promotion at the end of the action.

27. Positive action also includes positively assisting employees, or potential employees, who are disabled in line with the provisions of the Disability Discrimination Act.

Making a discrimination complaint

28. If an employee feels that they have been discriminated against they should use the grievance procedure, as set out in the grievance policy, to have their complaint investigated.

29. If the employee continues to be unsatisfied when the grievance procedure is exhausted they may make a claim to an Employment Tribunal, using the relevant discrimination questionnaires to help guide their claim. Further details are available on the websites of the Commission for Racial Equality, the Equal Opportunities Commission, the Disability Rights Commission and Employment Tribunal website.

(l) **Haras**
sment

30. Under the Protection from Harassment Act 1997, an individual must not pursue a course of conduct which amounts to harassment of another and which he or she knows, or ought to know, amounts to harassment of the other. An individual who pursues such a course of conduct may be guilty of a criminal offence and is liable on summary conviction to imprisonment or a substantial fine.

31. Harassment of any employee or third party at ORR by an employee will be considered a disciplinary offence irrespective of criminal or civil proceedings.

32. Harassment is behaviour that is unreciprocated, unreasonable, unwelcome or offensive. It might be targeted at an individual or at a group. It could be a single isolated event or persistent. It could be verbal, non-verbal, and/or physical. It includes a range of unsolicited behaviours which, whether intentional or not:

(a) create feelings of unease, humiliation, intimidation or discomfort; and/or

(b) cause offence, exclusion or withdrawal; and/or

(c) threaten, or appear to threaten, job security.

33. Some forms of harassment are obvious, such as physical assaults, demands for sexual favours or verbal threats or abuse. Others may be more subtle or less obvious, such a sexist or racist 'jokes', innuendo, displaying offensive material, or swearing. There is no simple definition. People find different things offensive, therefore if the recipient perceives the behaviour as harassment, then, by definition, the behaviour is harassment. Claims that there was no malicious intent do not negate the effect.

34. People react to harassment in different ways. The behaviour exhibited will vary depending on the length of time that the harassment has been going on, the seriousness of the incident (or incidences), and the ability of the individual to deal with it. However, people subjected to harassment may display some or all of the following prior to the problem being identified or a complaint made: repeated short term absences or poor timekeeping; marked deterioration in performance; becoming withdrawn, anxious, tearful or aggressive; loss of concentration; and/or low self esteem.

(m) **Bullying**

35. Bullying can be described as the persistent criticism and/or humiliation of individuals that undermines their professional confidence. It can manifest itself in a variety of different ways and may not be easily recognised. A manager may be bullying somebody that they manage, a colleague may be bullying one of their peers, a group may be bullying another individual, or an employee may be bullying their line manager.

36. Bullying is insidious and undermines the ability and confidence of the person who is suffering from it. It is usually persistent and often unpredictable. Bullying can lead to fear, demotivation, isolation, poor concentration, reduced performance, symptoms of stress and a high sickness absence level.

37. Quite often bullying may not be detected because victims are often unsure of their ground; they may blame themselves and think that they are in the wrong. Futhermore, unless it is blatant, the behaviour is often subtle and difficult to define and is often a combination of things not just one incident. Often there are no witnesses to bullying.

(n) **Victimisation**

38. Victimisation can encompass any situation where an employee complains of discrimination, harassment or bullying and the complainant's experience in the workplace is adversely affected by the handling of a complaint. If actions are taken or decisions made against the complainant that would not have been made in the absence of a complaint, this would contravene the anti-discrimination provisions of the discrimination legislation. The provisions are

wide enough to include situations where no complaint has actually been brought, for example, where the employer suspects that the individual is considering complaining.

39. ORR will not tolerate any victimisation, regardless of the nature of the complaint. Managers should ensure that in managing a complaint, no victimisation occurs. This arises when someone is treated less favourably than they would have been on grounds that:

(o) they have brought a complaint;

(p) it is known or suspected that they are contemplating bringing a complaint; or

(q) they are, or may be, assisting someone else with information in relation to a complaint; or

(r) a complaint has been made against them.

40. Managers should ensure that the parties to a complaint are kept fully aware of the outcome of any internal procedures. Complainants should not be ostracised or subjected to unusual duties - moving a complainant from their usual duties or treating them differently might give rise to a further complaint of victimisation. However, where a complainant finds it difficult to continue in their usual duties, or where it is impractical to keep the parties working together until the outcome of the complaint is known, then a change of duties to one or both of them may be considered. The Head of HR should be consulted before making such a decision.

(s) **Making a complaint about harassment, bullying or victimisation**

41. It is quite often a powerful measure for the employee to make it clear to the person concerned that their behaviour is unacceptable and that it should stop. If this is difficult or embarrassing the employee can tell the person how they feel in writing. Quite often, a polite request is enough to stop the harassment without the need for further action, particularly with less extreme examples of behaviour or comments. Once the person concerned has been told that their behaviour or comments are unwelcome, this may well be enough to stop it.

42. If an employee feels that they are unable to speak or write to the person directly or have done so and this has had no effect, they can make a complaint through the management line. This can be done either formally or informally using the grievance procedure. If the employee feels unable to speak directly to their line manager they should speak to their

countersigning officer or to a member of HR.

43. Additionally, the employee can speak to their Trade Union representative and/or make use of the Employee Advisory Service (EAS) (0800 282193) whose advisers will be able to provide support and advice. All contact with the EAS is confidential and they will not disclose any information given to them without consent unless:

(a) the EAS believes that ORR rules are being seriously breached (in these cases the EAS will firstly encourage the employee to speak to a member of HR or their line manager directly);

(b) a crime has been committed; or

(c) the employee or other staff are in danger.

44. If an employee is subjected to repeated incidents of harassment, bullying or victimisation they may find it useful to keep brief notes, detailing what has happened and when, and details of any witnesses. These notes will be an important aid to proceedings if action is taken at a later date.

(t) DIVERSITY

45. ORR recognises that managing diversity is complimentary to promoting equality because it ensures that individuals can reach their full potential and make a real contribution to the success of the organisation, even if they fall outside of the minority groups protected by equality legislation.

46. To ensure ORR is fair and make sound decisions, we consult widely and we employ and develop experienced and knowledgeable staff. In order to deliver fairness in the industry it is essential that each employee at ORR is able to process information from a diverse set of stakeholders, and arrive at the best and fairest decision. Our working practices and environment automatically leads itself to managing diversity and we do this well. But, to continue to deliver high quality outputs, ORR must ensure that it continues to improve and develop managing diversity.

47. ORR's work depends upon the ability of its staff to deliver thorough, constructive, timely and fair regulation. The more diverse we are as an organisation the more informed we will be in coming to conclusions because we will have wider understanding of potential issues and opinions when assessing the results of consultations. The mindset and skills of employees associated with consultation necessitate the ability to embrace the diversity of needs amongst the industry partners, for example when balancing the conflicting needs of freight and passenger capacity requirements.

48. ORR is heavily involved in influencing the development of EU railways policy and new legislation. The need to be able to embrace and manage diversity when working and negotiating in this area of work will help to ensure that Britain is a key partner is shaping the future of European railways.

(u) **Diversity initiatives**

49. We wish to continue to be an employer of choice, so that we remain able to retain the expertise we need to continue to excel as an organisation, through a high quality, motivated workforce. We recognise that, by valuing diversity, we will widen our pool of knowledge and learn different ways of undertaking business within a changing environment.

50. We must ensure that our employees are trained in diversity issues and we must develop an internal culture of embracing diversity so that it becomes second nature.

51. We also provide the following initiatives, that support the development of a diverse workforce above the needs of statutory minimum equality legislation:

(a) Investors in People accreditation;

(b) 'Two ticks' positive about disability accreditation;

(c) Occasional working from home policy;

(d) Flexible working policy;

(e) Flexitime Scheme;

(f) Parental, Paternity and Family Leave policy;

(g) Maternity and Adoption Policy;

(h) Subsidised Gym Membership Benefit;

(i) Annual leave and public and privilege holiday policy; and

(j) Domestic, compassionate and other special leave policy.

(v) MANAGEMENT AND CONTINUOUS IMPROVEMENT

(w) Equality and diversity action plan

52. The HR strategy will incorporate an equality and diversity action plan that is aimed to improve equality and diversity at ORR. The actions may include lawful positive action initiatives and will be informed by statistical monitoring and any legislative changes that affect the equality and diversity policy. There will be close ties with the ORR training strategy and programme due to the positive action approach to training.

53. The Head of HR will be responsible for the identification and management of all equality and diversity activities, and will be responsible for ensuring that employees are kept up to date with equality and diversity issues and are fully trained to fulfil their responsibilities.

(x) Monitoring

54. HR will undertake statistical monitoring to inform the equality and diversity strategy at ORR. The following areas will be monitored:

- Staff in post;
- Recruitment and selection;
- Performance management;
- Training;

- Promotion;

- Grievance and discipline cases; and

- Starters and leavers.

55. The information will be published in various media including HR activity reports, the ORR annual report and ad-hoc reports as presented to Directors Management Group.

(y) Changes to this policy

56. HR has the responsibility for ensuring the maintenance, regular review and updating of this policy. Revisions, amendments or alterations to the policy can only be implemented following consideration by Directors' Management Group and Staff Side, and approval by the ORR Board. Changes will be notified to employees when they occur.

(z) ANNEX A: ANTI DISCRIMINATION LEGISLATION

The following pieces of legislation make up the equality framework for working at ORR:

- Equal Pay Act 1970 and Equal Pay (Amendment) Regulation 1983

- Health and Safety at Work 1974

- Sex Discrimination Act 1975 (as amended)

- Race Relations Act 1976 and Race Relations (Amendment) Act 2000

- Trade Union and Labour Relations (Consolidation) Act 1992

- Disability Discrimination Act 1995

- Employment Rights Act 1996 and 2000
- Protection from Harassment Act 1997
- Human Rights Act 1998
- Maternity and Parental Leave Regulations 1999
- Disability Rights Commission Act 1999
- Part-time workers (Prevention of less favourable treatment) Regulations 2000
- Employment Equality (Religion and Belief) Regulations 2003
- Employment Equality (Sexual Orientation) Regulations 2003
- EU Law - Article 119 - Treaty of Rome and the Equal Pay and Equal Treatment Directives 1975 and 1976
- EC Law - Employment Directive (Article 13) 2000/78/EC
- The Equal Treatment Framework Directive requires the UK to implement national legislation preventing age discrimination in employment by 2006, however, as a public body, ORR is covered by the requirements of the directive now and must make steps to eliminate any age discrimination in our policies and practices now.

Security Manual Section 1.
SECURITY AT ORR

Introduction

1. This policy provides information on ORR's security standards and procedures. This guidance is not protectively marked but is issued for official use only.

Scope

2. This part of the security manual covers all ORR offices and applies to all staff and nominated contractors.

Responsibilities

3. All staff must be aware of the procedures and processes governing physical security. Particular responsibilities for handling security policy rest with the Departmental Security Officer (DSO), Information Technology Security Officer (ITSO) and Directors. Overall responsibility for this policy and its contents rests with the Departmental Security Officer (DSO)

Failure to comply with this policy

4. If you do not comply with this policy, you may be subject to disciplinary action which could lead to your dismissal.

Contacts

Senior Information Risk Owner (SIRO) – Tom Taylor

Departmental Security Officer (DSO) – David Phillips

IT Security Officer (ITSO) – Suzanne Hope

How Security is organised in ORR

5. As head of ORR, the Chief Executive has ultimate responsibility for security and its implementation within ORR. This responsibility is delegated to the DSO and the ITSO to:

(a) act as the link between the Cabinet Office and security organisations, interpreting threat assessments and liaising with the landlord and other tenants regarding the implementation of appropriate security measures.

(b) provide advice on the office's security and circulating guidance to staff and line managers (if required);

(c) audit and monitor the security policy implementation; and

(d) keep the Executive Committee (Exco) informed on security issues.

National Security levels (Please see appendix 4 for more details)

6. The ORR operates within the government threat assessment network.

7. This system is used to communicate the terrorist threat level. These assessments are provided as necessary by the security services and relate to the threat to the whole government estate. They are not specific to a building or department although can be varied to reflect local requirements dependent on intelligence received.

8. The response level will be changed as and when the threat increases or recedes, which will affect the security precautions implemented at individual locations.

9. You will be notified of changes to the security response as and when necessary. For information on the current assessment please go to the **Security** page on Orracle or follow the link to MI5 (**Threat levels explained**) or cabinet office for further information.

Action to be taken if you receive a bomb threats or alert

10. If you receive a call which you believe is a warning, you should aim to gather as much information as possible by;

a. making notes of what the caller said

b. listening to the background noise

c. noting any accent the caller may have had

d. time, length and source of the call (that is, if it came from an outside line)

e. and any other details that you can such as estimated age (child, young/old).

11. You should then relay the information as quickly as possible as detailed below;

(a) At Kemble Street, contact the local security team immediately (the number is 020 7413 6698), In Kemble Street any bomb threats or alerts will be co-ordinated by the local landlord's representative. They will consult tenants and the police, and decide what action to take in each case. Staff will be told what to do by network communications such as email, phone or word of mouth. It should be noted that the alarms are not sounded. Instead, a member of the facilities team will inform everyone of the evacuation procedure which will depend on the nature and location of the threat. Staff will not be evacuated unless instructed to do so by the police, responsible official or security.

(b) In the Glasgow office you will need to contact the police in the first instance using the 'local' direct line (the white phone) and repeat the details to them. The police will advise on any recommended action to take. Following this contact must be made with Tara House security and building manager.

(c) In the Birmingham office you will need to contact the police in the first instance using the 'local' direct line (the white phone) and repeat the details to them. The police will advise on any recommended action to take. Following this contact must be made with Ellison's helpdesk to contact the Facilities Manager.

(d) In Bristol you must contact the local security or facilities team (or both) immediately.

(e) In York and Manchester contact must be made with the on-site security team and the police by using the direct dial (white phone).

Information on suspect packages

12. Improvised Explosive Devices (IED) and Chemical/Biological (CB) devices can come in a variety of shapes and sizes. Although they may be large, they do not need to be bulky and can be in delivered packages or parcels. IED's in packages the size of paperback books have been among the more successful and in the case of courier delivered items, devices weighting in excess of 4kg have been used.

13. Staff who handle mail and parcels should be aware of the information contained in this document regarding the appearance and nature of suspect packages and it is would normally be expected that they would be the first to notice anything suspicious. It is however the responsibility of each member of staff to inform police or security if they believe that they are in receipt of a suspected package. Appendix 5 contains details of how to recognise a suspect device.

14. Please note that it is not necessary to open an envelope or package in any particular way to initiate an IED. It may be triggered by any attempt (however slight), to open the outer cover. If you are suspicious **do not** attempt to open it.

Further details contained in **Appendix 5**.

Duties of all staff

15. This section details the actions involved to maintain security and applies to all staff employed by the ORR. Staff with additional responsibilities are line managers, the Associate Director: Finance and governance, staff representatives and directors which are detailed later.

16. The following list contains the main responsibilities of all members of staff, including temporary staff (and line mangers must ensure that they are aware of this list);

(a) You are personally responsible for protecting information, documents and assets in your custody.

(b) All staff have legal responsibilities under health and safety legislation that also impact on security; for example, to take reasonable care of their own health and safety and that of others who may be affected by their actions or omissions (See the health and safety manual for more specific information on this topic).

(c) All staff are expected to co-operate in establishing safe and secure working conditions, procedures and practices.

(d) You must wear your identity badge or photo access control pass visibly with either a lanyard or belt clip, at all times when in government buildings.

(e) You must report the loss of your staff identity pass to your line manager and the facilities team/local accommodation team as soon as possible, who will arrange for a replacement. You will be required to complete a security report form.

(f) Wherever possible ensure that your desk is left clear of any OFFICIAL or protected documentation before you leave and that all vulnerable equipment is not left out overnight. It is your responsibility to ensure that all OFFICIAL and protected information and equipment is secured at the end of business each day.

(g) Protect all valuables (both personal and work related) and do not leave valuables unattended for long periods or overnight.

17. Acceptance of any gift or hospitality should be in accordance with the hospitality policy available on the intranet.

18. All employees have a responsibility to ensure that the integrity of the security management system of any office used is maintained. To this end staff must:

(a) ensure that no access points are made insecure by bolting or holding open for easy access;

(b) challenge all people entering the work area who are not recognised as having authority to be there; and

(c) report to the facilities team, local accommodation team and/or the security team any unauthorised visitors, unattended packages or bags, and suspicious behaviour both inside the building and around the perimeter of the complex.

19. Overall you are asked to be vigilant and all staff should ensure that any suspicious activity, particularly vehicle activity should be reported to your local security team and the police without delay.

20. At all locations line managers and staff must report any break-ins or suspected attempted break-ins, thefts, damage, etc., to the police, the local security or Facilities management team and to the ORR DSO.

Line managers: specific responsibilities

21. The following is a list of specific responsibilities allocated to line managers in addition to other general responsibilities detailed in this document. They must;

(a) make arrangements for checking that all access points to their work areas are secured at the start and close of business each day.

(b) ensure that the security procedures adopted are appropriate and are properly applied by their staff, and that the business conducted within their area of control is carried out in a secure manner appropriate to the risk.

(c) monitor the behaviour of individuals who have been given access to, or knowledge or custody of, protectively marked assets. Where doubt arises as to the continuing suitability of that individual to the role, a report should be made to the HR Manager.

(d) ensure that their staff meet their responsibilities with regards to ensuring their own security and safety and that of others.

(e) ensure that their staff handle all OFFICIAL and protectively marked material in accordance with section 2. of the security Manual and that documents are kept secure and are not left exposed.

(f) consider undertaking occasional checks after hours to ensure that information, assets and the building are secure.

(g) consider the security implications of allowing staff to work outside normal hours needs to be considered by line managers.

22. Line managers are also responsible making sure that no protected material is left out after working hours in their area of control.

Directors

23. Directors should ensure that all breaches of security (i.e. disclosure of information) in their directorate are reported as soon as possible to the DSO.

Associate Director, Finance and Governance: additional responsibilities

24. The Head of Finance has the following additional responsibilities:

(a) protecting the overall security of the Office's accounting systems;

(b) protecting the security of accounting standards and procedures;

(c) providing specialised advice and guidance on secure accounting practice; and

(d) providing the DSO with details of actual and potential accounting weaknesses and lapses.

25. Systems for the operation of tenders to obtain goods and services should be reviewed regularly with the above in mind.

Duties of the Departmental Security Officer (DSO)

26. The Departmental Security Officer (DSO) is directly responsible to the chief executive for co-ordinating all security matters within the office. Other responsibilities include:

(a) maintaining official liaison with the central security authorities; sending out alerts and receiving incident reports under the various reporting systems;

(b) developing security policies for the office;

(c) providing assurance on the implementation and adequacy of security measures throughout the office;

(d) providing advice and guidance on physical and document security; the personnel security policy and technical support to the operators of the vetting policy and service.

(e) initiating security assurance reviews when required and providing support for, or carrying out, the investigation of security breaches;

(f) providing advice about security procedures when required by internal customers;

(g) investigating reported security events including reporting back to directors and the Chief Executive as necessary. The chief executive will in turn brief the Board if appropriate.

27. The DSO is responsible for reporting major incidents to the Cabinet Office and the ITSO is responsible for reporting computer related incidents under the standard arrangements (including CPNI if necessary). Reporting incidents will be as defined in the Security Incident management good practice guide.

28. The DSO is responsible for making sure that security incidents are reported to the police as appropriate. They will also be responsible for liaison and obtaining information on threats from the local crime prevention officer.

29. The DSO will conduct checks from time to time (not just out of hours) and report any breaches of security to the individual and their line manager. Repeated breaches are referred up the line management chain. Depending on the circumstances, other staff or contractors may be advised (e.g. Capita if it is a computer related breach).

Duties of the Information Technology Security Officer (ITSO)

30. The Information Technology Security Officer (ITSO) is responsible for:

(a) providing technical advice and guidance on IT security matters;

(b) liaising with external IT security authorities;

(c) giving advice on the maintenance of the IT security policy;

(d) providing a centre of expertise for IT risk analysis;

(e) undertaking security reviews and audits where technical expertise is required;

(f) sending out alerts and receiving incident reports under the CPNI alert reporting system;

(g) reporting, through the DSO, on the state of IT security within the office;

(h) endorsing office IT security standards and procedures, approving guidance and promoting IT security training and awareness programmes;

(i) ensuring that information systems are operated within the overall framework of the GSI or PSN code of connection (There is additional responsibility for providing assurance on a regular basis that the organisation systems remain compliant);

(j) reviewing reports of IT security incidents within the office, and considering what further action may be required; and

(k) providing quarterly certificates of security assurance to the DSO, which will form part of the overall certificate of assurance given to the Chief Executive

Reporting and investigating breaches; all staff

31. If there is a breach, or suspected breach of security you should report the facts immediately to your director or head of section, who in turn should advise the relevant deputy, or the chief executive and the DSO who will co-ordinate any investigation. Following

consultation with the DSO the director or team leader should institute an immediate investigation to establish whether a loss or leak has taken place. The DSO should be given an oral report of the findings, supported by a written report as soon as possible.

32. Additionally, any breach of security that could be regarded as a potential disciplinary or dismissal matter is to be treated as a major case and the office's disciplinary procedures followed. Human Resources should be informed as soon as possible.

33. The manager discovering the breach or who has had reported a breach should consider and if necessary contact the police. They may seek advice from the DSO on the necessity of the action required. The DSO on being made aware of a breach ascertains what action in regards to the police has been taken.

34. Care must be taken to ensure that evidence uncovered of a security breach is preserved as part of the investigation.

Definitions

35. Breaches of security can be divided into: -

(a) LOSSES - where protectively marked or sensitive material or security keys are missing or there is reason to believe that such material or keys have been compromised; and

(b) LEAKS - when a report in the news media, or other information, gives rise to suspicion that there has been an unauthorised disclosure of protectively marked information.

36. The investigation of a leak may result in the discovery of a loss or vice versa, but normally, the procedure for dealing with the two types of breach are different.

Preliminary leak enquiries

37. Leaks normally take the form of reports in news media, which appear to involve the disclosure of sensitive official information. You should report any apparent leak immediately to the director or team leader who, in consultation with the DSO, will agree arrangements for immediate preliminary enquiries. The objective of the preliminary enquiry is to establish whether there is actually a leak or nothing more than an intelligent deduction or speculation by a journalist.

Full leak enquiries

38. How the investigation is progressed is a matter for agreement between the DSO and the senior manager involved. The Cabinet Office has a central panel of investigators for this sort of work and its services, or other professionals, may be utilised. The DSO has more details on how these matters are progressed.

Possibility of criminal proceedings

39. Investigators of breaches must bear in mind that an offence may have been committed, and therefore investigations must take place in a way that will not compromise any prosecution.

Possible legal action to recover documents or discover sources

40. If it should come to our attention that a media outlet has official information that has arisen from a leak, then swift action may be taken to obtain an injunction. This action should only be taken after consideration by the chief executive and with the agreement and assistance of the Cabinet Office security service. Similar consideration would have to be given to any attempt to obtain a court order upon a news provider demanding that they reveal their sources.

Outcome of security breach enquiries

41. At the completion of each enquiry, the security procedures must be reviewed to ensure that improvements are made to prevent a similar recurrence. The DSO will need to advise on and agree what further security measures are to be taken. All security breaches will be reported and discussed at the Security forum.

Security Forum

42. A security forum meets on a regular basis to review changes to security policy, security issues and to discuss and formulate recommendations following reported security breaches. This comprises of:

(a) Director Corporate Operations

(b) DSO

(c) ITSO

(d) A representative of Capita (our IT provider)

(e) A representative from the legal team

(f) Deputy Director, Railway Safety division

(g) And any other nominated person as necessary.

Appendix 1; Specific instructions relating to ORR run office locations

Security arrangements at One Kemble Street

1. OKS is made up of two buildings joined by a bridge link on the first and second floors. The normal site opening hours are 07.00 to 19.00, Monday to Saturday.

2. ORR occupies two floors (the second and the third) of 1 Kemble Street. It also holds the second floor bridge link and the second floor of CAA House. All work areas are protected by control access doors for access to and from common areas.

3. The site has a security presence 24 hours a day, 7 days a week. This is managed from a security control located in CAA house by a site supervisor monitoring full CCTV coverage of the perimeter of the building and some internal locations.

4. Apart from CCTV, other security measures, such as access control are in place. The level of security procedures is reviewed in light of specific intelligence and additional measures employed dependent on the nature of specific threats. This can be varied during times of heightened security such as restriction of visitors, bag searches etc. These changes to the baseline security procedures are done in conjunction between CAA and all the other tenants.

5. The security control room also monitors the fire control panels on the estate which all feedback into its main panel and computer. This room also acts as the point from which investigations take place if the alarm system is triggered and the emergency services are called if needed.

6. Security staff carry out regular internal walk round checks both in hours and out of hours (i.e. evenings, nights and weekends). These relate to checks for water leaks and the like, although they do check for evidence of intruders (This includes; evidence of forced access, checks of non-common areas including server room etc.).

7. Please ensure that ORR's meet and greet service at OKS is informed of any visitors that you are expecting. Any visitors not registered with the CAA reception (via 'Facilities') will be held at the downstairs reception until verified by the person that they are coming to see and collected.

Security at ORR Glasgow Office

8. Access to the Glasgow office is by using your access control photo pass via controlled door entry. These staff passes are issued by 'facilities' in London and operate the access control system to access the office. If your pass fails to release the door, then this should be reported to the Facilities Manager in London.

9. The main entrance to the building is open between the hours of 0730 to 1730. Access outside these hours can be gained either by using the landlord's proximity pass (issued only to those staff identified as requiring access outside normal working hours) or via the car park for those staff issued with a remote control sensor for operating the shutter doors.

10. Staff who have arranged access with a colleague outside these hours need to press button number 2 on the door entry system. This will alert the member of staff who can release the door lock.

11. Staff must not wedge open the door and be alert to non-invited guests trying to gain entry.

12. The access control system in Glasgow is linked to the main database located in One Kemble Street and any queries regarding the operation of the system should be referred to the DSO.

13. ORR is generally open between the hours of 0830 and 1700. Visitors should be instructed come to the 2nd floor (west) and press the buzzer for access. Staff should ascertain the purpose of the visit before allowing entry, if no prior notification has been received.

Security at ORR Birmingham office

14. The main entrance to the building is open between the hours of 0730 to 1900. Access outside these times is only available to staff in possession of a key. When the shutters are open access through the front door can be obtained by entering the code into the intercom or by ringing the office intercom phone.

15. Access to the Birmingham office on the third floor is by using a code entered into a digital keypad, or by pressing the inner intercom to gain access through the outer door into a shared corridor.

16. Your access control photo pass can then be used to access the office via controlled door entry. These staff passes are issued by facilities in London operate the control access into the office. If your pass fails to release the door, then this should be reported to the Facilities and Estates Manager in London.

17. Staff must not wedge open the door and be alert to non-invited guests trying to gain entry.

18. The access control system in Birmingham is linked to the main database located in One Kemble Street and any queries regarding the operation of the system should be referred to the DSO.

19. ORR is generally open between the hours of 0830 and 1700. Visitors should be instructed come to the front door at street level and press the buzzer for access. Staff should ascertain the purpose of the visit before allowing entry, if no prior notification has been received.

Security measures at other ORR offices

20. ORR staff are expected to acquaint themselves with and abide by local arrangements at their office. Security issues should be raised with the local facilities and/or security team on-site.

Appendix 2; ORR Access Control system

1. ORR has an access control system controlling access into its offices at One Kemble Street, Glasgow and Birmingham. This system is controlled from the security PC based in OKS. Passes are issued by facilities in OKS.

2. York, Manchester and Bristol offices all have controlled access door entry systems that are run by the local landlord and any queries regarding these systems should be referred in the first instance to the local security and/or facilities team.

3. At OKS each main tenant and the landlord utilise a control access system. Whilst these are similar there is no connection between them. Entry to the building for ORR staff and guests is either controlled by ground floor reception at OKS, who can issue paper passes, or by a proximity photo card system, using cards issued by ORR.

4. At OKS controlled access doors protect all the work areas on ORR's two floors. This system complements the landlord's system and is controlled by the Facilities team. All ORR staff and contractors are issued with a photo passes to allow access through these doors.

5. Temporary staff passes can be issued to staff who have forgotten their photo passes. These are issued for 24 hours and must be returned to issuer after that. There is a green official visitor's pass, which can be issued to external guests at the discretion of ORR Reception or designated person at Birmingham or Glasgow.

6. Everyone should carry an ORR pass of some sort whilst on ORR controlled premises. All passes are issued on a controlled basis and there are a few different types dependant on requirements. Normally access is not restricted by area or time.

7. ORR staff photo passes should work at OKS, Glasgow and Birmingham. If you have any difficulties using your pass please inform the facilities team in OKS.

8. Lost/Stolen passes should be reported to Facilities in London as soon as possible who will cancel the pass and re-issue a replacement. You will be required to complete a security incident form which should be sent to your line manager and the Information manager.

Type of Pass	Verification needed
• Staff Pass (personal issue, named photo)	SAM form – new starters, notification of loss/change of details all others
• Staff Pass (24 hours, temporary issue)	Facilities team issue on request.
• Contractors Pass (named photo for regular contractors)	
• Contractors Access pass (non-photo)	
• Official Visitors Pass	
• Consultants Pass (personal issue, photo pass)	Director/Deputy Director permission required. Issued by facilities

Table 1; Types of controlled access pass used on ORR system.

Appendix 3; Staff and contractor appointment, Vetting, Induction and Training

1. Checks need to be carried out to verify that potential workers are bona fide. The basic check is not a formal security clearance, and is designed to provide an appropriate level of assurance as to the trustworthiness and integrity of individuals.

2. The basic check should be carried out on all new permanent and fixed-term recruits, casual workers, long-term temporary workers and nominated contractors. The instructions are composed of the standard government-prescribed checks which relate to all government departments and agencies.

3. On appointment to ORR contracts, the procurement manager should discuss with the DSO if any contractors require to be put through the basic check procedure. Similarly if assurances can be obtained from the company concerned that they have been checked as part of a criminal records check (or similar) this will negate the need for this procedure to be applied.

Responsibilities

4. The responsibility for ensuring these checks are carried out rests with human resources (HR), line managers (for information), the DSO and the Procurement manager.

Stages in the Baseline Personnel Security Standard i.e. the basic check

5. In normal government terms, a basic check is designed for those employees whose work, in the main, involves uncontrolled access to, knowledge or custody of, government assets protectively marked up to and including SECRET on an occasional and need to know basis.

6. The check is known as the Baseline Personnel Security Standard. The Baseline standard comprises of the following stages; (between each stage, the information collected should be reviewed and assessed)

Stage 1 - identity check

7. An essential aspect of establishing the trustworthiness and integrity of an individual is confirming their identity – this check should be carried out before completing any of the other steps in the Baseline Standard.

8. The following information should be requested from the individual at this stage, and identifying documents provided for validation purposes:

(a) Full name;

(b) Date of birth;

(c) National Insurance number;

(d) Qualifications and educational details;

(e) Current permanent address.

7. The validation check will confirm that the following details are consistent throughout the information/documentation provided in paragraph 6:

(a) individual's full name and signature,

(b) date of birth,

(c) permanent address.

Stage 2 – employment history check

8. A check should be made to confirm that an individual has held the employment they claim – information on the last three years' employment (as a minimum) or academic history should be sought. Appropriate references can provide assurance, particularly where the reference is given by a reputable organisation or person known to ORR. Reasonable steps should be taken to ensure that the reference and referees are genuine, especially where the reference is less than convincing, for example being written on non-headed paper, or sent from a private email address. Referees should only be contacted with the individual's written consent.

9. If a second employment or academic reference is not available, a personal reference can be substituted, provided by a person of standing in the individual's community (e.g. a JP, medical practitioner, officer of the armed forces, teacher, lecturer, lawyer, bank manager, civil servant).

Stage 3 – nationality and immigration status check

10. All individuals are recruited according to government service nationality rules. It is important that an individual's nationality and their right to work in the UK are checked.

11. An individual should be asked to self-declare their nationality and their right to work in the UK. This information should be verified by checking one of the following documents:

(a) A UK passport describing the individual as a British citizen or citizen of the UK and colonies with the right of abode in the UK;

(b) A passport with a certificate of entitlement issued by the UK with the right of abode in the UK;

(c) A passport or ID card issued by European Economic Area (EEA) State, or State with an agreement forming part of the Communities Treaties (e.g. Switzerland) and which describes the holder as a citizen;

(d) An EEA registration certificate, permanent residence document or (permanent) residence card, or EEA residence permit (Swiss nationals are treated as EEA nationals for these purposes);

(e) A passport or travel document to show that the individual is exempt from immigration controls, with indefinite leave to enter or stay in the UK, or no time limit on the stay;

(f) An Application Registration Card (ARC) which indicates that the holder is entitled to take employment in the UK;

(g) A work permit or other approval issued by Work Permits UK and a passport or other travel document endorsed to show that the holder has current leave to enter or remain in the UK and is permitted to take the work permit employment in question, or a letter issued by the Home Office to the holder confirming the same.

Stage 4 – unspent criminal records

12. For the purposes of the Baseline Standard, the provisions of the Rehabilitation of Offenders Act (1974) apply. Individuals should complete an appropriate character declaration form detailing any "unspent" convictions. Individuals are not required to reveal "spent" convictions - certain criminal convictions are deemed to be "spent" after a prescribed period if an offender has remained free of convictions.

13. The character declaration will be verified via Disclosure Scotland, which is an independent organisation appointed by Cabinet Office to undertake security checks for all civil servants in the UK. Where "unspent" convictions are highlighted, the head of HR will consider the implications for ORR when deciding whether to proceed.

14. Individuals must provide the following original documents in order for the Disclosure Scotland check to be carried out:

(a) Valid passport/photo identity card (EU countries only) or original, full UK birth certificate issued within six weeks of birth

(b) At least two other forms of ID from the following (one MUST show the individual's current address):

- UK driving licence (photo card and paper)
- Proof of the individual's National Insurance Number (P45, P60, a payslip or a letter from a tax office or DSS which is no more than six months' old)
- Official documents containing the individual's current address (bank/credit statements, utility bills, benefit books etc.)

(c) If the individual has changed his/her name, the following will be required:

- Marriage certificate (married women only) or documentary proof of any other formal name changes (deed poll, divorce certificates etc.)

15. The following documents must not be accepted as proof of identity:

(a) duplicate or photocopied identity documents

(b) an international driving licence (as these are easily and frequently forged)

(c) a copy of a birth certificate issued more than six weeks after birth (as these can be purchased on request for any individual without proof of identity)

(d) an old British visitor's passport

Approving or refusing a basic check

16. In this organisation the head of HR approves or refuses the baseline standard check. Further guidance on refusing a check can also be obtained from the DSO.

Aftercare

17. Line managers are instructed to inform their HR Manager should doubts arise as to the as to the continuing suitability of that individual to given access to OFFICIAL documentation and protectively marked assets. A report should be made by the HR Manager concerned to the DSO.

Higher Level security clearance

18. The DSO will be in charge of all security clearance procedures higher than a baseline check.

19. Some posts such as the DSO, ITSO, the Head of Information are deemed to require security clearance to SC (security cleared) level. If you feel that you have a requirement to have individual members of staff security cleared please talk to the DSO for advice regarding this.

Appendix 4; Explanation of Threat levels

1. Threat levels are designed to give a broad indication of the likelihood of a terrorist attack. They are based on the assessment of a range of factors including current intelligence, recent events and what is known about terrorist intentions and capabilities.

Together with the detailed assessments behind them, this analysis informs security practitioners in key sectors and the police of the potential threat of terrorist attack. Threat assessments are also produced as necessary for individuals and events. There are five threat levels which inform decisions about the levels of security needed to protect the Critical National Infrastructure (CNI). The level of threat is monitored by the security services who publish the information on their website.

LEVEL	*DEFINITION*
LOW	An attack is unlikely
MODERATE	An attack is possible, but not likely
SUBSTANTIAL	An attack is a strong possibility
SEVERE	An attack is highly likely
CRITICAL	An attack is expected imminently

CAVEAT; Terrorism threat levels are designed to give a broad indication of the likelihood of a terrorist attack. They are based on the assessment of a range of factors including current intelligence, recent events and what is known about terrorist intentions and capabilities. This information may well be incomplete and readers should bear this in mind when making judgements on the basis of the threat levels. In particular, readers are reminded that SUBSTANTIAL and SEVERE both indicate a high level of threat and that an

attack might well come without warning.

Response Levels

3. Response levels provide a broad indication of the protective security measures that should be applied at any particular moment. They are set by security practitioners in Government and in some Critical National Infrastructure sectors. They are informed by the threat level but also take into account specific assessments of vulnerability and risk.

4. Response levels tend to relate to sites, whereas threat levels usually relate to broad areas of activity.

5. Within response levels, there is a variety of security measures that can be applied as appropriate. It is not intended that protective security measures for each Response Level should be determined by the Centre. Each site will have different protective security requirements depending upon not only threat but also location, vulnerability, likely impact on the business and the degree of acceptable risk.

6. Definitions are deliberately not prescriptive to allow security professionals to determine, in consultation with the National Security Advice Centre and Counter Terrorist Security Advisors, the appropriate level of protection.

7. There are three levels of response which broadly equate to threat levels as shown below:

LEVEL	*DEFINITION*
NORMAL	Routine baseline protective security measures, appropriate for our organisation, should be in place to protect staff/visitors/buildings. Should the threat rise consideration should be given to additional measures that are appropriate at each location. You may consider some precautionary measures worth deploying.
HEIGHTENED	A HEIGHTENED response level recommends consideration of additional protective security countermeasures above NORMAL to address the threat to our organisation, and will reflect specific operational and location vulnerabilities and the degree of acceptable risk in conjunction with other tenants. Measures deployed should be sustainable indefinitely; they may also be applied as a precautionary measure for a specific period.
EXCEPTIONAL	The EXCEPTIONAL response level requires consideration and implementation of maximum protective security

measures to minimise vulnerabilities and risk. Extra measures implemented are likely to be sustainable for a limited period only. Generally applies to specific buildings.

Appendix 5; Identification and action on receiving a suspect package

Acceptance of mail, parcels and packages into ORR at OKS

1. Collection by facilities staff from 'goods in' is the normal method of acceptance for all mail and packages into ORR.
2. All packages and mail should be sorted in the ORR post room because if there is found to be a suspicious package it can be dealt with more effectively at that location.
3. Ground floor 'Goods in' provides the first stage check for received mail and packages into ORR. If on going to goods in you deem an ORR package to be suspect do not bring it up to ORR, leave it alone and highlight it to goods in and security staff.

How to Spot Suspicious Letters or Packages; All offices

4. A letter or package should be treated is suspicious if one or more of the following is true:

- Has any powdery substance on the outside
- The package has been posted abroad, is unexpected or from someone unfamiliar to you
- Has excessive postage
- It is addressed using incorrect titles or titles with no name, or has misspellings of common words
- Handwritten or poorly typed address The writing or typing is sloppy or uneven
- Is addressed to someone no longer with ORR or is otherwise outdated
- Has no return address, or has one that can't be verified as legitimate
- Is of unusual weight, given its size, or is lopsided or oddly shaped
- Has been wrapped in an unusual amount of tape
- Is marked with restrictive endorsements, such as "Personal" or "Confidential"
- Shows a city or location in the postmark that does not match the return address
- The package has Oily stains, discolorations or strange odours.
- The package has protruding wires or aluminium foil or has a ticking sound.
- Packaging includes visual distractions, e.g. indications that you have already won £50,000.

Handling of all packages

5. Common sense and care should be observed when inspecting and opening all mail or packages:
   - Examine (feel) unopened envelopes for foreign bodies or powder.
   - Do not open letters with your hands; use a letter opener.
   - Open letters and packages with a minimum of movement to avoid spilling any contents.
   - Consider additional precautions such as wearing gloves and restricting the opening of mail to a limited number of trained individuals.

What to Do with a Suspicious Letter or Package

6. If think that you may have a suspect package, do not try to open it, but isolate it and follow the relevant procedure below.
   - Handle the package with care and do not shake or empty the contents of anything deemed to be suspicious.
   - Do not sniff, touch, taste, or look closely at it or any contents that may have spilled.
   - Do not carry the package or envelope, show it to others, or allow others to examine it.
   - Isolate the letter or package using gloves to put it into the plastic bin where provided or put the package or envelope on a stable surface.
   - Close doors and windows to the room where the package is.
   - Alert others in the area about the suspicious package or envelope (in OKS confer with other members of the facilities team or failing that alert Security). Please note you may find it helpful to speak to the intended recipient to check that it is not something that they have ordered for delivery at work.
   - It is expected that Security should contact the emergency services through use of the 999 procedure.
   - Once the package is confirmed as suspicious arrange to leave the area, close any doors, and take actions to prevent others from entering the area.
   - If possible shut off the ventilation system and evacuate others in the area
   - Dispose of any normal mail that you do not open that may have become contaminated.

- Wash hands with soap and water to prevent spreading potentially infectious material to face or skin.

- If possible, create a list of persons who were in the room or area when this suspicious letter or package was recognised and a list of persons who also may have handled this package or letter. Give the list to both the local public health authorities and the fire brigade or police when they arrive.

Other do's and don'ts

- Do not allow children to open mail
- Keep mail away from food preparation areas
- If your clothes are contaminated, carefully remove them and isolate them

If possible contact the delivering postal organisation or shipping service.