

leading resolutions

Leading Resolutions Limited

and

xxx

**Master Services Agreement
For The Provision of
Consultancy Services**

MASTER SERVICES AGREEMENT FOR THE PROVISION OF CONSULTANCY SERVICES

This Agreement is made on **xxx** ("Commencement Date")

BETWEEN

Leading Resolutions Limited, whose company number is 04307011, whose registered office is at 2 Coped Hall Business Park, Royal Wootton Bassett, SN4 8DP ("Leading Resolutions")

AND

xxx, whose company number is **xxx**, whose registered office address is **xxx** (the "Company").

BACKGROUND

- (A) Leading Resolutions has a requirement for consultancy services to be provided to its clients by consultants engaged by Leading Resolutions.
- (B) The Company engages personnel with the required levels of skills and experience and is willing to provide such consultancy services to the clients of Leading Resolutions.
- (C) This is a framework agreement that will govern the provision of any such consultancy services.
- (D) This Agreement is to be interpreted consistently with these Background paragraphs, which form an integral part of this Agreement.

1 DEFINITIONS

In this Agreement, the following expressions have the following meanings:

"Agreement" means this Master Services Agreement ("MSA") and each Project Statement. In the event of any conflict of meaning between this Agreement and any Project Statement, the express provisions of that Project Statement shall prevail.

"Authorised Representative" means the person named by either party, as notified in a Project Statement, who is vested with the authority of the appointing party to communicate all of that party's decisions to the other party in connection with the Services, and who will act as the prime point of contact with the Authorised Representative of the other party authorised to receive the decisions of the other party in connection with the Services.

"Client" means Leading Resolutions' customer as identified in the applicable Project Statement.

"Contract" means the agreement entered into between Leading Resolutions and the Client.

"Data Protection Legislation" means the General Data Protection Regulation (EU/2016/679) and the Data Protection Act 2018 and any successor legislation to

leading resolutions

either. "Personal Data", "Data Controller", "Data Processor", "Data Subject" and "Process" are all as defined in the Data Protection Legislation.

"Deliverables" means all artefacts designed, developed, written or prepared by the Company (whether alone or jointly with Leading Resolutions or any other independent contractor of Leading Resolutions or any Client on whatever media) and all related documentation, including but not limited to any specification, project plans, presentations, designs, dashboards, programs, data, reports, and all other written materials or computer output, produced in the course of providing the Services.

"Personnel" has the meaning given to it in clause 2.1.

"Proprietary Rights" means all intellectual property rights including but not limited to copyright, confidential information, rights in computer programs, patents, design rights, trademarks, service marks, registered designs, applications for any of those rights, trade and business names, unregistered trade and service marks, know-how, database rights and rights of the same or similar effect or nature as the foregoing in each case in any jurisdiction.

"Project Statement" means a written and signed description of a Project (including the Services) as agreed between Leading Resolutions and the Company deemed to form a Schedule to this Agreement and to be incorporated in it.

"Project" means any work to be undertaken for a Client.

"Protected Parties" means all Clients and other third parties who may receive the direct or indirect benefit of the Services, as end user or other beneficiary including a customer of any Client.

"Services" means specific identified services to be provided by the Company and its Personnel in relation to a Leading Resolutions' Project for its Client as more particularly described in the Project Statement.

"Working Day" means a day (other than a Saturday, a Sunday or public holiday) on which banks in London are open for non-automated banking business.

2 SERVICES

- 2.1 In respect of each supply of Services under an agreed Project Statement, the Company agrees to provide the Services to Leading Resolutions together with any other tasks from time to time that may be agreed in writing between the parties and shall provide the Deliverables as described in accordance with the applicable Project Statement and the terms and conditions of this Agreement. The Person(s) named in the Project Statement (the "Personnel") shall be the initial Person(s) utilised in the performance of the Services but may include substitutes utilised by the Company in accordance with clause 5.2.
- 2.2 Either party may request changes to the Services or any other aspect of any Project Statement or this Agreement. Change requests must be supported by sufficient detail to enable the other party to assess the impact of the proposed change on the cost, timetable or any other aspect of the Agreement. Both parties agree to work together to consider and, if appropriate and with the agreement of the Client, agree any changes. Until a change is agreed in writing by the parties, both parties will continue to act in accordance with the latest agreed version of the Agreement and/or the Project Statement.
- 2.3 This Agreement is not an exclusive arrangement and accordingly:
 - (a) subject to the restrictions on disclosure of information and the Company's other obligations in this Agreement, the Company is not required to provide Services

leading resolutions

exclusively to Leading Resolutions (but shall not undertake any engagement or activity on its own account or for any other company or business which directly competes or presents a conflict of interest with or may be detrimental to the interests and operation of Leading Resolutions business activities from time to time in business areas in which the Company has performed or is performing consultancy assignments, without the written consent of Leading Resolutions (such consent not to be unreasonably withheld), whilst any Project Statement is current and for a period of 6 months (or such longer period expressed in the Project Statement) after the completion of the Services required by such Project Statement); and

(b) Leading Resolutions may engage any third party at any time to provide services to Clients that are the same as or similar to the Services.

2.4 For the avoidance of doubt this Agreement does not oblige either party to enter into a Project Statement with the other. Leading Resolutions is not obliged to offer the Company any works at any time, likewise the Company is not obliged to accept any such offer of works which shall be made. The Company is not obliged to make its services available at any time.

3 DELIVERABLES

3.1 The Company will ensure that the Personnel perform the Services and prepare and deliver to Leading Resolutions the Deliverables with all reasonable skill and care and in a professional manner and in accordance with any timetable set out in the applicable Project Statement.

3.2 The Deliverables will be accepted by Leading Resolutions on the terms of the Project Statement and subject to them meeting the acceptance criteria set out in the Project Statement. Such acceptance not to be unreasonably withheld by Leading Resolutions.

4 TERM AND TERMINATION

4.1 This Agreement commences on the Commencement Date shown and shall continue unless terminated in accordance with clause 4 of this agreement.

4.2 This Agreement may be terminated immediately by notice in writing:

(a) by Leading Resolutions, if the Company or any member of the Personnel, in the reasonable opinion of the Client, other Protected Party or Leading Resolutions, renders unsatisfactory performance; is in wilful breach or neglect of duty; does not comply with the legal rules and regulations in respect of health and safety, data protection and security applicable to independent consultants; does not comply with generally accepted behaviour expected of a consultant or other on site visitor; uses drugs or alcohol such as to impair performance or which jeopardises the interests of Leading Resolutions or the Client or otherwise behaves in a manner which would tend to bring Leading Resolutions or the Client into disrepute or adversely affect their respective businesses. In the event that the right to terminate under this clause is exercised within the first 30 days of any Project Statement, the Company accepts that Leading Resolutions is entitled to withhold any payment due in respect of Services provided during such period as compensation for any losses, cost and liabilities incurred by Leading Resolutions;

(b) by either party at any time if the other is in material or continuing breach of its obligations under this Agreement and (in the case of a breach capable of

leading resolutions

remedy) fails to remedy the breach within a period of 10 Working Days after the service of written notice by either party;

- (c) by either party if the other convenes a meeting of its creditors or if a proposal shall be made for a voluntary arrangement within Part I of the Insolvency Act 1986 or a proposal for any other composition, scheme or arrangement with, or assignment for the benefit of, its creditors, or if the other shall be unable to pay its debts within the meaning of Section 123 or Section 268 of the Insolvency Act, 1986 or if a trustee, receiver, administrative receiver or similar officer is appointed in respect of all or any part of the business or assets of the other, or if a petition is presented or a meeting is convened for the purpose of considering a resolution or other steps are taken for the winding up of the other, or for the making of an administration order (otherwise than for the purpose of a voluntary amalgamation or reconstruction) or for the placing of the other into administration pursuant to Schedule B1 to the Insolvency Act 1986;
 - (d) by Leading Resolutions if the Contract or the applicable part of the Contract or the applicable Project is terminated by the Client for any reason whatsoever;
 - (e) by Leading Resolutions in circumstances where the Company is not able to provide the Services and cannot provide a substitute in accordance with clause 5.2;
 - (f) by Leading Resolutions if the Company or any Personnel present, in the reasonable opinion of Leading Resolutions, a conflict of interest;
 - (g) by either party for convenience by giving notice in writing in accordance with the "Notice Period" specified in the Project Statement and if a Notice Period is not specified in the Project Statement, on 5 Working Days' written notice.
- 4.3 Any termination of this Agreement under this clause 4 shall be without prejudice to any other rights or remedies of either party under this Agreement or at law and will not affect any accrued rights or liabilities as at the date of termination.
- 4.4 Any termination of this Agreement for any reason whatsoever shall have the effect of terminating any respective Project Statement unless agreed otherwise between the parties.

5 THE COMPANY'S OBLIGATIONS

As an independent business the Company is responsible for its own provision of services and methodology. The Company, including any individuals utilised by the company in the performance of the Services, shall not be subject to control (or any right of control) by Leading Resolutions or its Client, as to the manner in which it performs the Services.

The Company agrees to:

- 5.1 Provide the Services in a timely and efficient manner, using reasonable skill and care, and to a professional standard which will conform to the standards generally in the industry for similar services and to remedy promptly and free of charge any work which is rejected by Leading Resolutions or the Client, or reported by Leading Resolutions to be defective. The Company also warrants that it and its Personnel will comply with all applicable laws and legal regulations in the performance of its obligations under this Agreement.

leading resolutions

- 5.2 Utilise suitably qualified and experienced Personnel to provide the Services to Leading Resolutions during the term stated in the Project Statement. The Company may utilise a substitute in place of any initially named Personnel, at any time for any reason, and will ensure that such substitute possesses the necessary skills, qualifications and experience to perform the Services agreed in the Project Statement. The Company shall arrange at the Company's expense for substitutes to review any documentation and attend such meetings as might be necessary to ensure continuity of the Services.
- 5.3 Insofar as they are applicable to independent contractors, ensure conformity by all Personnel with Leading Resolutions' or the Client's health and safety rules and procedures, information systems and social media policies and standards, security practices and confidentiality obligations whilst on Leading Resolutions, the Client's and or any other third party's premises provided that the same have been notified in writing to the Company and procure that all Personnel shall at all times act in a lawful and proper manner.
- 5.4 Insofar as they are applicable to independent contractors, ensure all Personnel comply with the IT security policy of Leading Resolutions at Schedule A (as amended by Leading Resolutions from time to time) relating to the use of their own or the Company's devices in the provision of the Services and any other IT security measures Leading Resolutions may specify from time to time, and indemnify Leading Resolutions in relation to all losses, costs, damages and liabilities arising from any breach of the policies by the Personnel.
- 5.5 Insofar as they are applicable to independent contractors, conform with any and all Client or Leading Resolutions policies and procedures in relation to the submittal and authorisation of status and or service reports, invoicing and payment. Failure to comply with such policies and procedures may result in the withholding of payment to the Company.
- 5.6 Duly instruct and give all necessary directives (especially as to the time, place, type and performance of work) to and control its Personnel in order to ensure an efficient and professional performance of the Services.
- 5.7 Notify Leading Resolutions of absence of Personnel other than planned absence (leave) on the first day of the absence.

6 LEADING RESOLUTIONS' OBLIGATIONS

Leading Resolutions agrees to:

- 6.1 Provide the Company promptly with such information and documents as might reasonably be required for the performance of the Company's obligations under this Agreement.
- 6.2 Provide reasonable guidance, administrative support and assistance in relation to the Deliverables.
- 6.3 Pay for the Services in accordance with the terms of this Agreement.

7 WORKING ARRANGEMENTS

- 7.1 The Company's and Leading Resolutions' Authorised Representatives will meet to discuss and review the Services from time to time and the outcome of such meeting shall be agreed in writing.

leading resolutions

- 7.2 The Personnel assigned to perform the Services will remain under the overall control of the Company at all times during the term of this Agreement.
- 7.3 The Company will use all reasonable endeavours to replace promptly any Personnel who leave the Company or who are absent through illness or incapacity, in accordance with clause 5.2.
- 7.4 Nothing in this Agreement shall constitute any Personnel an employee, worker, or agent of Leading Resolutions or any Client and the Company shall be fully responsible for and shall indemnify Leading Resolutions and every Client for and in respect of:
- (a) any income tax, national insurance and social security contributions and any other liability, deduction, contribution, assessment or claim arising from or made in connection with either the performance of the Services or any payment or benefit received by the Personnel in respect of the Services, where such recovery is not prohibited by law, except where the Company has been notified that the Project falls within the scope of IR35 in which case it shall be the obligation of Leading Resolutions to deduct income tax and National Insurance upon payment of the Company's invoice. The Company shall further indemnify Leading Resolutions and every Client against all reasonable costs, expenses and any penalty, fine or interest incurred or payable in connection with or in consequence of any such liability, deduction, contribution, assessment or claim;
 - (b) any liability arising from any employment-related claim or any claim based on worker status (including reasonable costs and expenses) brought by any Personnel arising out of or in connection with the provision of the Services.
- 7.5 Leading Resolutions may at its option satisfy such indemnity (in whole or in part) by way of deduction from payments due to the Company.
- 7.6 The Company warrants that it is not, nor will it during the term of this Agreement, become a managed service company, within the meaning of section 61B of the Income Tax (Earnings and Pensions) Act 2003.

8 PROPRIETARY RIGHTS

- 8.1 All Proprietary Rights in the Deliverables are to be owned by Leading Resolutions. The Company assigns (including by way of present assignment of future copyright) all such rights to Leading Resolutions, immediately upon the coming into existence of such rights.
- 8.2 The Company warrants to Leading Resolutions that all current Personnel and future Personnel are the responsibility of the Company and that it has obtained from all current Personnel (and will obtain from all future Personnel before they are appointed to deliver the Services) a written and valid assignment of all existing and future Proprietary Rights created by the Personnel, whether alone or jointly with others, in the course of their employment with, or contractual engagement by, the Company and of all materials embodying such rights, and that the Personnel have agreed to hold on trust for the Company any such rights in which the legal title has not passed (or will not pass) to the Company. The Company will ensure that the Personnel utilised to perform the Services under each Project Statement waive in favour of Leading Resolutions any moral rights and author's rights and rights of a similar nature that they may have in the Deliverables. To the extent the use of the Deliverables by Leading Resolutions or any Client requires the use of the Company pre-existing intellectual property rights the Company grants Leading Resolutions a non-exclusive, worldwide, royalty free and perpetual licence to make or provide such use and agrees that such licence may be transferred or sub-licensed to the Client at the discretion of Leading Resolutions.

leading resolutions

- 8.3 At the request and expense of Leading Resolutions, the Company shall do all such things and sign all documents or instruments reasonably necessary in the opinion of Leading Resolutions to enable Leading Resolutions to obtain, defend and enforce its rights in the Deliverables.
- 8.4 Upon request by Leading Resolutions, and in any event upon expiration or termination of this Agreement, the Company shall at its expense promptly deliver to Leading Resolutions all copies of the Deliverables then in the custody, control or possession of the Company.
- 8.5 The provisions of this clause 8 shall survive the expiration or termination of this Agreement.
- 8.6 The Company undertakes to keep the Deliverables confidential and not to make copies of them available to any third party for any purpose without prior agreement in writing from a director of Leading Resolutions.

9 INTELLECTUAL PROPERTY RIGHTS INDEMNITY

- 9.1 The Company shall on demand indemnify Leading Resolutions and each Client and their respective officers and employees against all liability, claims, costs (including legal costs), expenses and other losses arising from or in connection with any actual or alleged claim or action brought by any third party in respect of any infringement of any Proprietary Rights ("Claim"). Leading Resolutions shall notify the Company of any Claim and the Company shall at its own expense support Leading Resolutions and/or the applicable Client(s) as may be required for the defence against such Claim. The Company will reimburse any final judgment including all reasonable attorneys' fees entered against Leading Resolutions and/or the applicable Client(s) and any settlement between Leading Resolutions and/or the Applicable Client(s) and the relevant third party with respect to any Claim.
- 9.2 If any part of the Deliverables should become the subject of any Claim, or if a Court judgment is made that the Deliverables do so infringe, or if the use or licensing of any part of the Deliverables is restricted, the Company at its option and expense may:
 - (a) obtain for Leading Resolutions and the applicable Client(s) the right to continue to use the Deliverables; or
 - (b) replace or modify the Deliverables so that they become non-infringing provided that, in any such case, this modification does not have an adverse effect on the capabilities and/or characteristics and/or qualities of the Deliverables.
- 9.3 The Company will have no liability under this clause to the extent that it arises from:
 - (a) any combination or interfacing of the Deliverables with other work or materials not supplied by the Company; or
 - (b) modification of the Deliverables unless the modification was made or approved expressly by the Company.
- 9.4 In any case, the above indemnity will not be construed as an exclusive remedy or as a limitation of (i) the liability of the Company or (ii) Leading Resolutions' right to obtain from the Company any indemnification for damages, for which Leading Resolutions is entitled pursuant to Clause 13 below.

leading resolutions

- 9.5 The parties intend that each applicable Client should be able to enforce the provisions of this clause 9 against the Company under the Contracts (Rights of Third Parties) Act 1999.

10 FEES AND EXPENSES

- 10.1 In consideration of the Services rendered by the Company pursuant to a Project Statement, on receipt of a valid undisputed invoice and a completed timely electronic timesheet record, Leading Resolutions will pay to the Company fees in the amounts and on the commercial terms set out in the Project Statement, once supported by authorised Client time sheets/expense reports in a form acceptable to Leading Resolutions which will be submitted weekly to the Leading Resolutions Authorised Representative.
- 10.2 All expenses incurred by the Company will be for the account of the Company. Only by way of exception Leading Resolutions may on occasion authorise specific expenses to be reimbursed via prior written agreement with Leading Resolutions and as detailed in the Project Statement, at cost via a properly supported invoice from the Company provided to Leading Resolutions. Occasions may arise when the Personnel use a car for business purposes associated with Leading Resolutions work. The Company shall ensure that at all times the vehicle has relevant motor insurance policies (including for business use) and shall cover all costs associated for such use.
- 10.3 VAT shall be paid additionally at the prevailing rate in respect of fees and pre-agreed expenses, subject to production of a valid VAT invoice.
- 10.4 Unless otherwise agreed in the Project Statement, such fees will accrue monthly and the Company will render monthly invoices for each calendar month to Leading Resolutions in respect of the fees and commits to submitting a valid monthly invoice no later than the first Working Day of the following calendar month. Failure to comply with this clause may result in the withholding of payment to the Company.
- 10.5 Subject always to clause 10.4, all fees payable by Leading Resolutions shall be payable within 30 days from date of receipt of a valid undisputed invoice and approved timesheets from the Company, unless otherwise stated in the Project Statement. If Leading Resolutions disputes any portion of an invoice Leading Resolutions will notify the Company within 15 Working Days of receipt of such invoice and the dispute will be referred to the Dispute Resolution procedure in clause 17.9 of this Agreement.
- 10.6 The Company shall have the right to suspend the provision of Services if any part of an undisputed payment is not received by the due date provided the Company gives Leading Resolutions 14 days' notice of such intention to suspend and further provides Leading Resolution the same period to make payment.
- 10.7 The fees payable in relation to the Services provided by the Company is a confidential matter between the Company and Leading Resolutions. Without prejudice to clause 11, the Company shall not, and shall procure that the Personnel shall not, discuss such fees with the Client or any other Protected Party, any other third party or any member of Leading Resolutions staff without the prior written consent of Leading Resolutions. Failure to comply with this clause will be treated as material breach of this Agreement that is not capable of remedy and which justifies termination of this Agreement in accordance with clause 4.2(b).
- 10.8 The Company agrees not to increase fees or rates in respect of Services to be provided to a Client once agreed with Leading Resolutions. The Company also agrees to hold fees and rates through any contract renewal up to a period of 12 months, unless there

leading resolutions

is, in the reasonable opinion of Leading Resolutions, a significant change to the Services or Deliverables undertaken.

- 10.9 Payment will only be made in respect of days actually worked by the Company and Services actually supplied in accordance with this Agreement generally and the Project Statement specifically. Payment in full or in part of any invoice shall be without prejudice to any claims or rights of Leading Resolutions or the Client against the Company or the Personnel in respect of the provision of the Services.

11 CONFIDENTIAL INFORMATION

- 11.1 Except as required by law each party undertakes to the other that all information obtained from the other which is either stated to be confidential or could reasonably be regarded as confidential ("Confidential Information") disclosed to it by the other party in connection with this Agreement or which may at any time come into the other party's knowledge possession or control (including, in the case of the Company, any information of a confidential nature relating to the Client and each Protected Party and each Project) shall not be used for any purposes other than those required or permitted by this Agreement and shall not be disclosed to any of the Personnel or any third party except insofar as this may be required for the proper operation of this Agreement and then only under appropriate confidentiality provisions approved by the other party.
- 11.2 The Company undertakes to each Client and other Protected Party (and the parties intend that each Client and other Protected Party shall be entitled to enforce the provisions of such undertaking against the Company under the Contracts (Rights of Third Parties) Act 1999) that no Confidential Information relating to a Client or other Protected Party or to a Project disclosed to it in connection with this Agreement or which may at any time come into its knowledge, possession or control shall be used for any purposes other than those required or permitted by this Agreement or disclosed to any third party except insofar as this may be required for the proper operation of this Agreement and then only under appropriate confidentiality provisions approved by the Client or other Protected Party.
- 11.3 The obligations of confidentiality set out in this clause 11 shall cease to apply to any particular item of Confidential Information once it becomes public knowledge other than by a breach of confidence, but shall survive the termination or expiry of this Agreement and of any Project, Project Statement or Contract.
- 11.4 The Company will return all Confidential Information, property and materials (including Deliverables) made available to the Personnel by Leading Resolutions or the Client in connection with the Services upon termination of the applicable Project, Project Statement, Contract or this Agreement or upon request by Leading Resolutions at any time and such information and materials shall not be copied, published or used for any purpose other than the performance of the Services. The Company shall, and shall procure that the Personnel shall, immediately upon termination of the applicable Project, Project Statement, Contract or this Agreement or upon request by Leading Resolutions at any time irretrievably delete any information relating to the Client, any other Protected Party and/or the Project and/or Leading Resolutions stored on any magnetic or optical disk or memory and all matter derived from such sources which is in its or possession or control or that of the Personnel. For the avoidance of doubt this includes confidential contact details of business contacts made during each Project Statement but excludes information held on personal social or professional networking accounts.

leading resolutions

12 EMPLOYMENT RESTRICTION

- 12.1 Whilst this Agreement is in force and for a period of twelve months from its termination for whatever reason, neither party will employ or offer employment to any person employed by or acting on behalf of the other party who was assigned to provide services in connection with this Agreement in the preceding twelve months (a "Restricted Person").
- 12.2 If either party is in breach of Clause 12.1, that party (recognising that the other party will suffer substantial damage) will pay to the other party by way of liquidated damages, and not by way of penalty, a sum equal to 35% of the total of that person's starting annual salary or other remuneration.
- 12.3 The Company agrees that it will not, and will procure that the Personnel will not, for the term of this Agreement and for the 6 month period from its termination for any reason, either directly (through employment or direct contract by the Client of the Personnel) or indirectly (under a contract of service through the Company or through any third party) provide the Services provided (or similar to those provided) under this Agreement to any Client to which Leading Resolutions has introduced the Company and its Personnel ('Introduced Client') or other Protected Party except by contract through Leading Resolutions or by the Company paying to Leading Resolutions a fee of 50% of the total remuneration agreed to be paid for the services by the Introduced Client (or other Protected Party) for the relevant period of supply.

13 DATA PROTECTION

- 13.1 The Company and Leading Resolutions acknowledge that for the purposes of the Data Protection Legislation, Leading Resolutions is a processor of data belonging to their Clients and the Company is the data sub-processor.
- 13.2 The Company and Leading Resolutions will comply with the Data Protection Legislation.
- 13.3 The Company shall, and procure that its Personnel shall, in relation to any Personal Data processed in connection with a Project or any Services:
 - 13.3.1 Process that Personal Data only in fulfilment of this Agreement or on written instructions of Leading Resolutions.
 - 13.3.2 Keep the Personal Data confidential.
 - 13.3.3 Comply with Leading Resolutions' reasonable instructions with respect to processing Personal Data and process Personal Data only in so far as is necessary to provide Services or comply with the Company's obligations under this Agreement or required by law.
 - 13.3.4 Not transfer any Personal Data outside of the UK or European Economic Area without Leading Resolutions' prior written consent.
 - 13.3.5 Assist Leading Resolutions in responding to any data subject access request made to the Client and to ensure compliance with its and the Client's obligations under the Data Protection Legislation with respect to security, breach notifications, privacy impact assessments and consultations with supervisory authorities or regulators.
 - 13.3.6 Notify Leading Resolutions without undue delay on becoming aware of a Personal Data breach or communication which relates to the Data Protection Legislation.

leading resolutions

- 13.3.7 At the written request of Leading Resolutions, delete or return Personal Data and any copies thereof to Leading Resolution on termination of the Agreement unless required by the Data Protection Legislation to store the Personal Data.
- 13.4 The Company shall ensure that it has in place appropriate technical or organisational measures to protect against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to Personal Data appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures. Such measures may include, where appropriate:
 - 13.4.1 Pseudonymising and encrypting Personal Data.
 - 13.4.2 Ensuring confidentiality, integrity, availability and resilience of its systems and services.
 - 13.4.3 Ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident.
 - 13.4.4 Regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by it.
- 13.5 The Company shall within 24 hours, or earlier if practicable, of becoming aware, notify Leading Resolutions in writing of any breach of security leading to the accidental or unlawful destruction, loss, alteration, disclosure or access to Personal Data. The notice provided will specify:
 - 13.5.1 the categories and number of individuals and records concerned;
 - 13.5.2 the likely consequences of the breach;
 - 13.5.3 any steps taken to mitigate and address the breach; and
 - 13.5.4 specify an appropriate person for us to contact about the breach.
- 13.6 The Company will provide reasonable information requested by Leading Resolutions in relation to such a breach,
- 13.7 In relation to Personal Data Processed by the Company under this Agreement, the Company shall co-operate with Leading Resolutions and the Client to the extent reasonably necessary to enable Leading Resolutions to adequately discharge its responsibility as a data processor under Data Protection Legislation (including in respect of the preparation of data protection impact assessments).
- 13.8 Leading Resolutions shall have the right to audit the Company and relevant records and materials as necessary to demonstrate the Company's compliance with its obligations under this Agreement and Data Protection Legislation. At any time the Company will co-operate fully to allow and assist such audits, including on-site inspections of its business premises or processing facilities, conducted by Leading Resolutions or their auditor.

leading resolutions

14 INSURANCE AND LIABILITY

- 14.1 Nothing in this Agreement shall operate to limit or exclude either party's liability for: (i) personal injury or death caused by its negligence; (ii) breach of the obligations in section 12 of the Sale and Goods Act 1979; or (iii) fraud.
- 14.2 The Company shall indemnify Leading Resolutions and each Client for any loss, liability, costs (including legal costs), damages or expenses arising from any breach by the Consultant or any Personnel of the terms of this Agreement including any negligent or reckless act or statement, omission or default in the provision of the Services and shall accordingly maintain in force during this Agreement full and comprehensive insurance policies of the types and values specified below with a reputable insurer or insurers authorised to underwrite such risk in the UK:
- Public Liability of at least £2,000,000
Professional Indemnity Insurance of at least £1,000,000
(the "Insurance Policies").
- 14.3 The Company shall on request supply to Leading Resolutions and/or the Client copies of the Insurance Policies and evidence that the relevant premiums have been paid.
- 14.4 The Company shall comply with all terms and conditions of the Insurance Policies at all times. If cover under the Insurance Policies shall lapse or not be renewed or be changed in any material way or if the Company is aware of any reason why the cover under the Insurance Policies may lapse or not be renewed or be changed in any material way, the Company shall notify Leading Resolutions without delay.
- 14.5 The Company shall ensure that all monies receivable in respect of any insurance effected in accordance with this Clause 13 shall be applied in making good the loss or damage in respect of which such monies are receivable. The Company shall bear the cost of all exclusions and limitations under the insurances and shall pay for any excess.

15 MODERN SLAVERY

- 15.1 In performing its obligations under the Agreement, the Company shall:
- (a) Comply with all applicable anti-slavery and human trafficking laws, statutes, regulations from time to time in force including but not limited to the Modern Slavery Act 2015; and
 - (b) Not engage in any activity, practice or conduct anywhere in the world, that would constitute an offence under sections 1,2 or 4, of the Modern Slavery Act 2015 if such activity, practice or conduct were carried out in the UK;
- 15.2 The Company represents and warrants that at the date of this agreement and, to the best of its knowledge, neither the Company nor any of its officers and/or employees has been convicted of any offence involving slavery and human trafficking nor has been or is the subject of any investigation, inquiry or enforcement proceedings by any governmental, administrative or regulatory body regarding any offence or alleged offence of or in connection with slavery and human trafficking.
- 15.3 Leading Resolutions conducts its business in a manner that is consistent with its internal policies and has in place an Anti-Slavery and Human Trafficking policy and action plan.

leading resolutions

16 ANTI BRIBERY

The Company shall, and shall procure that the Personnel shall:

- 16.1 comply with the Bribery Act 2010 and all other applicable laws, statutes, regulations, and codes relating to anti-bribery and anti-corruption (**Relevant Requirements**);
- 16.2 have and shall maintain in place throughout the term of this Agreement its own policies and procedures to ensure compliance with the Relevant Requirements and will enforce them where appropriate;
- 16.3 promptly report to Leading Resolutions any request or demand for any undue financial or other advantage of any kind received by the Company in connection with the performance of this Agreement;
- 16.4 immediately notify Leading Resolutions in writing if a foreign public official becomes a partner, officer or employee of the Company or acquires a direct or indirect interest in the Company, and the Company warrants that it has no foreign public officials as direct or indirect owners, partners, officers or employees at the date of this Agreement.

17 GENERAL CONTRACT PROVISIONS

- 17.1 This Agreement supersedes any previous contracts or agreements between Leading Resolutions and the Company, which shall be deemed to have been discharged by mutual consent.
- 17.2 This Agreement, incorporating each Project Statement, constitutes the entire agreement between the parties. Each party confirms that it has not relied upon any representation not recorded in this Agreement inducing it to enter into this Agreement. No variation of this Agreement will be valid unless confirmed in writing by the Authorised Representatives of each party on or after the date of this Agreement.
- 17.3 All clauses relating to license and ownership, confidentiality, warranties, non-exclusivity, non-solicitation and waiver shall survive the termination or expiry of this Agreement.
- 17.4 No forbearance or delay by either party in enforcing its respective rights will prejudice or restrict the rights of that party and no waiver of any such rights or of any breach of contractual terms will be deemed to be a waiver of any other right or of any later breach.
- 17.5 The relationship between Leading Resolutions and the Company is that of independent contractors. Neither party is agent for or partner with the other, and neither party has any authority to make any contract, whether expressly or by implication, in the name of the other party, without that party's prior written consent and only then for express purposes connected with the performance of this Agreement.
- 17.6 Any notice given under this Agreement shall be in writing and shall be delivered by hand or by commercial courier or by Royal Mail special delivery posted in the United Kingdom. In the case of commercial courier or Royal Mail special delivery, delivery shall be deemed to take place on receipt by the sender of a notice that the addressee has "gone away" or refused to take delivery or any notice having similar effect. Notices shall be delivered or posted to the addresses of the parties given above or to any other United Kingdom address notified in substitution on or after the date of this Agreement.
- 17.7 Neither party may assign this Agreement or any benefits or interests arising under this Agreement without the prior written agreement of the other party which will not be

leading resolutions

unreasonably withheld or delayed, provided that Leading Resolutions may assign this Agreement to any purchaser of all or of a substantial part of Leading Resolutions' business and undertaking.

- 17.8 Any Client or other Protected Party may enforce clauses 9, 11.2 and 13 of this Agreement in accordance with the Contracts (Rights of Third Parties) Act 1999 ("the Act"). Subject to the foregoing, no other person or entity who is not a party to this Agreement shall have any right under the Act to enforce any term of this Agreement, but this does not affect any right or remedy of a third party which exists or is available apart from the Act. The parties reserve the right under section 2(3)(a) of the Act to rescind, terminate or vary this Agreement without the consent of any Client or other Protected Party.
- 17.9 Both parties agree to attempt in good faith to resolve any dispute or claim arising out of or in connection with this Agreement or any Project Statement promptly through negotiations between the Company's senior executives and Leading Resolutions' management. If the matter is not resolved by negotiation, the parties will refer it to mediation in accordance with the Centre for Effective Dispute Resolution ("CEDR") Model Mediation Procedure. (See www.cedr.co.uk). Unless the parties agree on the choice of mediator within 7 days of one party nominating a proposed mediator in writing to the other, the mediator shall be appointed by CEDR at the request of either party. If the parties fail to agree terms of settlement within 42 days of the start of the first meeting held under such procedure, the dispute may be referred to litigation by either party. Nothing in this clause shall prevent or delay either party from seeking injunctive relief in any court in respect of any infringement of intellectual property or breach of confidence or from joining the other party to any proceedings issued against the first party by a third party.
- 17.10 This Agreement shall be construed and governed by English law and the parties submit to the exclusive jurisdiction of the English courts to settle any dispute (including non-contractual disputes or claims) arising from or connected with this Agreement, including a dispute regarding the existence, validity or termination of this Agreement or the consequences of its nullity.
- 17.11 The Company undertakes that after termination for whatever reason of this Agreement it and its Personnel will not represent themselves as being in any way connected with Leading Resolutions or any Client or other Protected Party.
- 17.12 No party shall be liable for any failure to perform its obligations under this Agreement, if such failure results from any act of God, riot, war, civil unrest, terrorism, flood, severe weather conditions, earthquake, or other causes beyond such party's reasonable control (including any mechanical, electronic, or communications failure, but excluding failure caused by a party's financial condition or negligence).

18 EQUIPMENT TOOLS, MATERIALS, AND / OR SUPPLIES

- 18.1 The Company shall supply, at the Company's sole expense, all necessary off-site equipment, tools, materials and / or supplies to perform the services. Equipment must be fit for purpose and to a standard reasonably expected of a professional consultancy. Leading Resolutions will not provide any tools or equipment, including mobile phones or PC and office equipment. Leading Resolutions will not fund, or make any contribution toward, any Company expenses directly or indirectly attributable to any Project.

leading resolutions

SIGNED FOR AND ON BEHALF OF xxx		SIGNED FOR AND ON BEHALF OF Leading Resolutions Limited	
Signature:		Signature:	
Printed name:	xxx	Printed name:	Tracey Coleman
Company Role:		Title:	Operations Manager
Date:		Date:	

leading resolutions

Schedule A

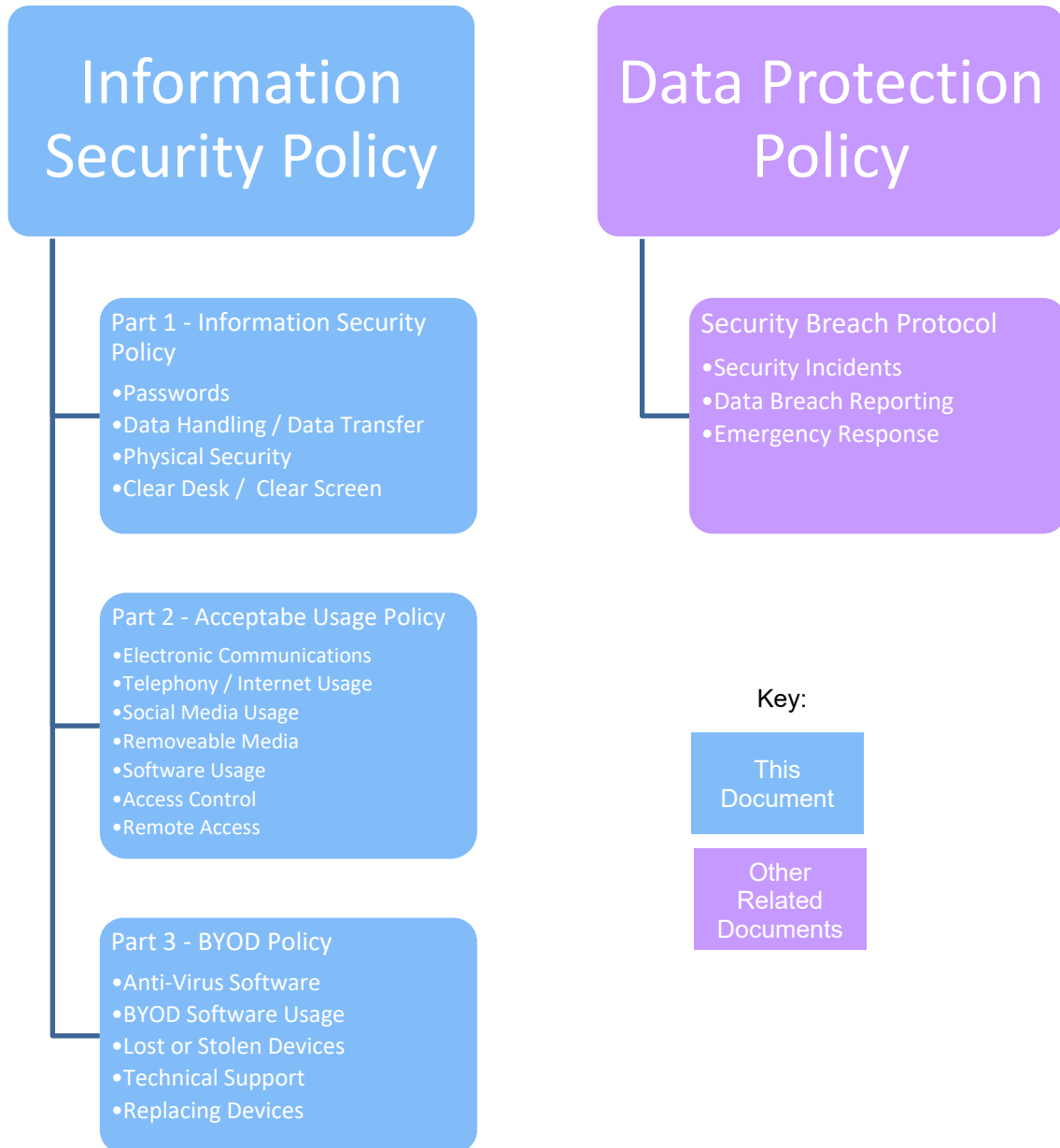
Leading Resolutions

Information Security Policy

leading resolutions

Foreword and Scope

There are several parts to this Information Security Policy. Together, along with the technical security controls provided by our outsourced IT Partner Onecom Limited (“our IT Partner”) they make up the Information Security Management System (ISMS) for Leading Resolutions. The structure of this policy suite is as follows:



Introduction

Our IT and communications systems are intended to promote effective communication and working practices within our organisation. This policy outlines the standards you must observe when using our IT and communications systems and similar systems belonging to us or our clients (together “IT systems”) and the circumstances in which we may monitor your use of IT systems.

leading resolutions

This policy covers all employees, consultants, contractors and anyone who has access to our IT systems (“Workers”).

The purpose of this policy is to protect the IT system and company data, and to prevent company data from being deliberately or inadvertently lost, disclosed or altered, while enabling you to access our systems using a device. This policy sets out the circumstances in which we may monitor your use of the IT system, access your device and the action which we will take in respect of breaches of this policy.

Misuse of IT Systems or breach of this policy can damage the business and our reputation and may lead to us revoking your access to our systems, whether through a device or otherwise. It may also result in the termination of the engagement between you and Leading Resolutions, or in some cases, it may lead to possible criminal charges. You are required to co-operate with any investigation into suspected breach, which may involve providing us with access to devices and any relevant passwords and login details.

Leading Resolutions’ objectives for the policy suite are to:

- Support organisational objectives
- Impose controls in line with Leading Resolutions’ acceptable level of risk
- Meet applicable statutory, regulatory, contractual and professional duties
- Protect the interests of individuals and other key stakeholders.

To increase security compliance standards Leading Resolutions workers undergo a vetting and checking procedure including credit and identity checking, verification of employment references and where required, DBS checks. They are also all subject to confidentiality clauses within their contracts.

Partners and third parties working with or for Leading Resolutions, who may have access to our IT systems, will be expected to read, understand and comply with this policy. No third party may access Leading Resolutions IT Systems without having first entered into a data confidentiality agreement, which imposes compliant standards of conduct and which gives Leading Resolutions the right to audit compliance with the agreement.

If you have any queries or concerns about the application of this Information Security Policy, please contact hello@leadingresolutions.com for advice and guidance.

Roles and Responsibilities

The Board of Directors and all those in managerial or supervisory roles throughout Leading Resolutions are responsible for developing and encouraging good information handling practices within the organisation.

The Senior Information Risk Owner is accountable to the Board of Directors. This accountability includes Information Security risk management and compliance with this policy.

The Data Protection Advisor role reports to the Senior Information Risk Owner and has specific responsibilities in respect of monitoring for compliance, providing training

leading resolutions

and being the first point of call when seeking clarification on any aspect of Information Security compliance.

Compliance with this policy is the responsibility of every Leading Resolutions worker. It is also the worker's responsibility to ensure that any contravention of this policy is reported quickly and honestly.

Contact Information

Throughout this policy, where you see references to the following roles, you may use the following contact information:

Head Office – hello@leadingresolutions.com

Our IT Partner – ITMSservices@onecom.co.uk

Data Protection Advisor – maria.mccoy@leadingresolutions.com

Senior Information Risk Owner – jon.bance@leadingresolutions.com

Compliance with Policy

Compliance with this policy is assured in 3 ways:

- Awareness and training about information security best practice and policy is mandatory for all Leading Resolutions employees. This training forms part of the induction programme and will be refreshed annually.
- Technical controls and monitoring applied by our IT Partner
- Annual due diligence security questionnaire issued to all Leading Resolutions associate consultants to confirm their understanding of and adherence to corporate policy
-

PART 1 – Information Security Policy

Passwords

Leading Resolutions O365 accounts require complex passwords that must be a minimum of eight (8) characters and should contain a combination of letters, numbers and special characters.

In addition, Leading Resolutions also employ multi-factor authentication for O365, using the Microsoft Authenticator App.

All IT equipment used outside our office but with access to the IT systems must be secured with a PIN number, strong password, or biometric security checking (such as a fingerprint reader). You must keep PINs and passwords confidential and change them regularly. You must not use another person's username and password or make available or allow anyone else to log on using your username and password.

leading resolutions

Words, names, birth dates, addresses, postcodes, telephone numbers, or any other easily guessed combination should not be used. User IDs and passwords must not be written down or kept within the general area of the computer.

If someone demands a password, refer them to this document or have them contact Head Office to explain the requirement.

User passwords must not be inserted into email messages or other forms of electronic communication. An exception to this is for password protected documents, in which case passwords should be sent through a separate channel of communication from the password protected document (such as by text or given verbally).

New applications should enforce the user to change the password after initial login. If this is not enforced through an application, always change your password on first use, when signing up for new services, or client systems.

If an account or password is suspected to have been compromised, report the incident to Head Office and change all passwords immediately.

Data Handling

All corporate information is owned by Leading Resolutions. You should not delete, destroy or modify existing systems, programs, information or data on or forming part of the IT system.

All Leading Resolutions workers are responsible for ensuring that any personal data which Leading Resolutions holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by Leading Resolutions to receive that information and has entered into a confidentiality agreement.

Personal data should be:

- Kept in a locked filing cabinet (with the key secured)
- Kept in a locked drawer (with the key secured)
- If computerised, password protected
- Stored on (removable) computer media which are encrypted

When connected to Leading Resolutions' IT system, you must not download or install software from external sources without authorisation from Head Office. This includes software programs, instant messaging programs, screensavers, photos, video clips and music files. If in doubt, staff should seek advice from our Head Office.

You must not attempt to gain access to restricted areas of our IT network, or to any password-protected information.

When using your own IT equipment linked to the IT system, you will take such precautions as we may require against importing viruses or compromising system security. The system contains information which is confidential and/or subject to data

leading resolutions

protection legislation. More information about the use of your own devices can be found in PART 3 – BYOD Policy.

All corporate records must be maintained in line with the corporate retention policy.

Personal identifiable data stored and processed by Leading Resolutions workers must adhere to the standards described in the Data Protection Policy suite.

Corporate data can be printed out, producing a paper copy. Paper documents that contain commercially sensitive data must be stored securely and disposed of by secure shredding.

Do not use a device to capture images, video, or audio, whether native to the device or through third-party applications, within the client's workplace as this requires consent. If there is a significant project requirement to do so, consult with the Data Protection Advisor about how to obtain specific and informed consent.

Hard drives of redundant Company PCs must be removed and destroyed before disposal.

Data Transfer

A mutual NDA must be in place between Leading Resolutions and any third parties before any information exchange takes place. These NDAs should be a standard document, emphasising the ownership and responsibilities of each party regarding the data/information assets.

Commercially sensitive or personal data being sent by email must be encrypted using password protection. The password should be sent through a separate channel of communication from the password protected document (such as by text or given verbally).

Physical Security

Leading Resolutions workers must ensure that all computer assets (computers, monitors, laptops, printers etc.) that are regularly used by them are maintained and used in a manner such that the possibility of damage or loss is minimised. Damage to or loss of computer caused by negligence and/or violation of this policy may result in the responsible party being charged for the repair or replacement costs.

Equipment must never be left unattended in locations such as airports and hotel lobbies. Leaving mobile devices with company data on them unattended may result in revocation of BYOD privileges.

You should restrict physical access to workstations to authorised personnel only and secure workstations (screen lock or logout) prior to leaving area to prevent unauthorised access.

You must enable a password-protected screen saver with a short timeout period (maximum 5 minutes) to ensure that workstations will be protected. Our IT Partner will automate this wherever possible.

leading resolutions

Mobile devices must be positioned so that they (and the information contained within them) are not visible from outside a ground-floor window. Additionally, you should ensure that monitors are positioned away from public view. If necessary, install privacy screen filters or other physical barriers to public viewing.

Protected data processing areas such as Server rooms must be secured with key or passcode access.

All visitors to buildings must follow visitor access control procedures as determined by the organisation. For Leading Resolutions, this entails buzzing on the access panel and being met in reception, but client sites may have additional sign-in protocols and security passes.

Clear Desk/Clear Screen

The desktop on all workers computers should have the approved Leading Resolutions branded wallpaper.

Users should log off their machines when they leave the workstation.

Where practically possible, paper and computer media must be stored in suitable locked safes, cabinets or other forms of security furniture when not in use, especially outside working hours.

Where lockable safes, filing cabinets, drawers, cupboards etc. are not available, office/room doors must be locked if left unattended. At the end of each session all sensitive information must be removed from the workplace and stored in a locked area. This includes all personal identifiable information, as well as business critical information such as salaries and contracts.

Sensitive information, when printed, must be cleared from printers immediately.

Removing printed information from desks reduces the risk of damage or destruction from a disaster such as fire, flood or explosion.

Make sure any office paper is disposed of using the locked confidential waste bin if it contains personal or commercially sensitive data.

Do not print off emails to read them. This generates an increased clutter and risk. Consider scanning paper items and filing them on the server, in the correct location.

Always clear your desktop before you go home.

PART 2 - Acceptable Usage Policy

Email and Electronic Communications

All emails or messages created or sent, using Leading Resolutions user accounts are the property of Leading Resolutions.

We monitor communications systems for the purpose of evaluating system performance, virus detection, unauthorised use, compliance with policies, legislation

leading resolutions

and industry regulations. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.

We reserve the right to retrieve, delete or block access to emails, messaging systems or attachments in the interests of security.

You must not reveal your email or logon passwords to anyone.

You must exercise extreme caution in downloading and executing any files attached to email. If the email or attachments are not clearly business related or are from unknown sources, they must never be opened or executed. If you wish for an attachment to be investigated, notify Head Office who can forward to our IT Partner.

Please always be vigilant for phishing emails to your Leading Resolutions email address, and take the following 3 actions:

1. DO NOT CLICK ANY LINKS!
2. Report it to Head Office (hello@leadingresolutions.com)
3. Delete the phishing email

Refer to the **Security Breach Protocol** for additional guidance on phishing emails.

If you receive any electronic communications that are intended for someone else, you must delete the message and notify the sender immediately. If the email contained personal or commercially sensitive information, this should also be reported to Head Office (hello@leadingresolutions.com) as a potential data breach.

Where confidential information is exchanged, only use 'Reply to All' if every recipient of the original message requires a response. You must not auto-forward Leading Resolutions email messages to external email accounts.

You must not subscribe or register to any web services using your Leading Resolutions email address, if those services are not directly relevant to your assigned duties.

Although email is a vital business tool, you should always consider if it is the appropriate method for a particular communication.

You must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or otherwise inappropriate electronic messages.

You should take care with the content of all electronic messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Emails should be spell checked before sending and remember that you have no control over where your email may be forwarded by a recipient. Avoid saying anything which would cause offence or embarrassment if it was forwarded to third parties or found its way into the public domain. Humour and sarcasm can be easily misinterpreted and should be avoided.

Email and instant messages are required to be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not

leading resolutions

mean that messages cannot be recovered for the purposes of disclosure. All electronic messages should be treated as potentially retrievable.

Telephony

Personal and corporate mobile phones are both permissible – please see the PART 3 - BYOD Policy for guidance on using your own devices.

Corporate mobile phones will only be issued to employees where deemed appropriate.

Use of SMS messaging must comply with the electronic communications section above, in PART 2 of this policy.

All mobile phones must have PIN, passcode or biometric security controls enabled as a minimum to prevent unauthorised access.

All corporate mobile phones are owned by Leading Resolutions. When the phone is returned after use it must be in a reasonable condition.

If a corporate or personal mobile phone is lost or stolen, you must report it to Head Office.

Personal use of corporate phones is allowed within reason. The user should avoid extended or overseas personal calls or calls to high-cost telephone lines.

Internet Usage

We reserve the right to monitor internet usage (including pages visited and searches made) as reasonably necessary, for evaluating system performance, to monitor whether usage is legitimate and in accordance with this policy, and to assist with the prevention and detection of criminal activities. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.

Leading Resolutions provides access to the internet to support the needs of the business. Using a Leading Resolutions computing device or network connection to access the internet for non-work purposes (e.g. checking home email, online shopping, social media etc.) is permitted, providing it does not interfere with your duties or contravene Leading Resolutions policies.

Websites considered dangerous or inappropriate may be automatically blocked. Categories of website considered dangerous or inappropriate include but are not limited to: hacking, malicious software (malware), pornography, race hate, terrorism and illegal activities.

You must not attempt to access websites that are likely to be dangerous or inappropriate. Computers can be infected by viruses and malicious programs by just visiting a webpage.

Inform our Head Office immediately if you suspect your computer may have a virus.

leading resolutions

Leading Resolutions copyrighted content (including images, videos and other digital content) must not be uploaded to the internet without approval from the Senior Information Risk Owner.

Images, articles and other material downloaded from the internet must only be used or shared as defined by their copyright licensing terms and conditions.

Social Media and Internet Forums

An internet forum is a web application for holding discussions and posting user generated content. Internet forums are also commonly referred to as Web forums, message boards or Social Media.

When posting content to such forums, using Leading Resolutions accounts or systems, you must ensure that your personal beliefs and opinions cannot be construed as those of Leading Resolutions. Whenever your affiliation with Leading Resolutions is known, you must clearly state "the opinions expressed are my own and not necessarily those of Leading Resolutions". Note however that this does not apply if you are posting officially sanctioned messages as part of our brand strategy.

Removable Media

Removable media includes devices such as external hard drives, USB flash drives, DVDs, MP3 players and smartphones. They may be connected via the USB port, infra-red connection, Bluetooth or in any other way.

The use of removable media should only occur for trusted or security-controlled devices, as they are one of the highest risk sources for malware.

Removable media that is used for storing or processing any company data may only be used where it is encrypted/password protected. This is to reduce the risk that confidential or personal data may fall into the hands of unintended recipients, if that removable media is lost or stolen.

Software Usage

Without the prior written authorisation, users shall not:

- Install any unlicensed or unapproved software on Leading Resolutions owned equipment
- Install Leading Resolutions owned software on any third-party computer equipment
- Provide copies of Leading Resolutions owned or licensed software to anyone
- Engage in any acts of software piracy

Our IT Partner shall ensure that all software installed or utilised on our IT System is properly licensed.

Access Control

All user access rights will incorporate the principle of least privilege which grants the lowest level of access, rights, privileges and security permissions needed for the performance of duties.

leading resolutions

All user access requests for accessing any internal applications must be requested and authorised by Head Office.

Leading Resolutions exercises a formal user registration process for all network users, permanent and temporary. This process is part of the induction and includes the submission of checklists to the IT function to setup appropriate access rights.

Access to an account during absence by another member of staff must be authorised by the Senior Information Risk Owner. Where such access is granted, the original user must immediately change their password, upon their return to work.

In the case of any user resignation or termination or a move between departments or projects, the HR Administrator or Project Lead must make the request to remove or change the access rights. There is also a full exit process that must be followed to ensure that client confidential data is deleted or handed back, and that valuable IP is captured, at the end of a project or employment contract.

User accounts will be audited and reviewed annually by appointed system owners, under the guidance of the Data Protection Advisor.

Wherever possible, all privilege user access should be integrated with two-factor authentication.

Users with privileged access will have two user IDs: one for normal day-to-day activities and one for performing administrator duties. Administrators may only use their administrator account to perform administrator functions.

All privileged user access activity should be logged and monitored.

Users with privileged access must always be aware that these privileges place them in a position of considerable trust. Users must not breach that trust by misusing privileges or failing to maintain a high professional standard.

Remote Access/Wi-Fi

The wireless network (Wi-Fi) within the Leading Resolutions Head Office comprises a guest and internal network connection. Both are secure connections.

The user shall not expect any privacy while using our wireless network because it may be subject to monitoring, with cause, for security, legal, or troubleshooting purposes. This may include monitoring for bandwidth usage, security related incidents and compliance, or a request from legal/law enforcement authorities.

Network capacity is limited. If your device connection to Wi-Fi uses excessive bandwidth, sends disruptive signals, or violates any other Information Security Policies, it will be subject to limitations or possible disconnection.

As most internal Leading Resolutions systems are cloud based, remote access is enabled as standard and additional log-in details are required for each system.

Users will adhere strictly with all applicable policies while using any Wi-Fi network to access Leading Resolutions systems and accounts, such as the Internet and Social Media sections of the PART 2 - Acceptable Usage Policy.

leading resolutions

When using client Wi-Fi provisions, all workers should read and respect the client information security policies and processes.

PART 3 – BYOD Policy

This policy applies to workers who use a personal device including any accompanying software or hardware (referred to as a 'device' in this policy) anywhere in the world in relation to services provided to Leading Resolutions for its clients.

This policy applies to all devices used to access our IT systems, which may include (but are not limited to) smartphones, mobile or cellular phones, tablets, and laptop or notebook computers.

You must pay for your own device costs under this policy, including but not limited to voice and data usage charges and any purchase and repair costs.

When you access the IT systems you may be able to access data about us or our group companies, clients, distributors, suppliers and other business connections, including information which is confidential, proprietary or private. The definition of data is very broad, and includes all written, spoken and electronic information held, used or transmitted by us or on our behalf, in whatever form (collectively referred to as "company data" in this policy).

When you access the IT system using a device, we are exposed to a number of risks, including the loss or theft of the device (which could result in unauthorised access to our systems or company data), the threat of malware (such as viruses, worms, spyware, Trojans or other threats that could be introduced into our systems via a device) and the loss or unauthorised alteration of company data (including personal and confidential information which could expose us to the risk of non-compliance with legal obligations of confidentiality, data protection and privacy). Such risks could result in damage to our systems, our business and our reputation.

Anti-Virus Software

All PCs and devices must use standard, up to date, licensed, anti-virus software installed and scheduled to run at regular intervals. This software is to remain activated at all times.

Anti-virus software must be configured to automatically start up so that it is running before devices are connected to our IT systems, or the internet.

Although users are expected to maintain their own devices, Leading Resolutions must be notified of any threats to information security. Therefore, the user must inform our Head Office if they suspect their devices are infected, if they are alerted by the anti-virus software, or if there is any out-of-ordinary behaviour of their computer or applications.

Virus-infected devices must be removed from the network until they are verified as virus-free.

BYOD Software Usage

leading resolutions

Users must ensure that they maintain their device operating systems by installing application updates as they become available.

Users may download and install applications from the platform's (e.g., Apple's, Android's) public application store, as long as the application complies with this Information Security Policy and our **Data Protection Policy**. If there is any doubt, please speak to our Data Protection Advisor.

Users must ensure that applications provisioned by themselves and used for work purposes are properly licensed.

Users should understand that unmanaged or unapproved applications constitute a security risk. Where there is any doubt, refer decisions for installing new software applications to Head Office.

We reserve the right to install an enterprise-procured Mobility Management software agent, or any other software deemed necessary, on the user's device.

Lost or Stolen Devices

In the event of a lost or stolen device, or where you believe that a device may have been accessed by an unauthorised person or otherwise compromised, you must report the incident to Head Office immediately. There is a **Security Breach Protocol** that must be followed which is part of the Data Protection Policy suite.

Users may be required to cancel any individual voice and data services or change the password details for various cloud services or client accounts.

Leading Resolutions will not be responsible for reimbursing the cost of a lost or stolen device.

Personal Data

Personal data is any data that can identify (is unique to) an individual, such as name, email address, phone number etc. We have a legitimate basis on which to access and protect company and client data stored or processed on your device, including the content of any communications sent or received from the device. Our lawful basis for processing is documented in our Record of Processing Activities.

You must be aware of our and your obligations under the relevant data protection legislation when processing company or client data. You must ensure that company or client data is used only for the business purposes for which it was intended, and that you do not use it for a purpose different from that for which it was originally intended.

You should also minimise the amount of company and client data you retain on your device by accessing information remotely where possible, storing project information on SharePoint and deleting any data saved locally on your device as soon as it is no longer required.

You must take reasonable steps to minimise loss of your personal data on your device, although we shall not be responsible for any such loss that may occur.

leading resolutions

Please refer to the **Data Protection Policy** suite or the Data Protection Advisor if you have any questions pertaining to the protection of personal data.

Additional Security Requirements

In addition to the above, you must:

- At all times, use your best efforts to physically secure the device against loss, theft or use by persons who we have not authorised to use the device. You must secure the device whether or not it is in use and whether or not it is being carried by you. This includes, but is not limited to, passwords, encryption, and physical control of the device
- Comply with our device configuration requirements
- Adhere to the device Password Policy in PART 1 of this Policy
- Maintain the device's original operating system and keep it current with security patches and updates. Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing out systems or company data
- Prohibit use of the device by anyone not authorised by us, unless you can ensure that they are using a segregated account and will abide by this Policy in full
- Not alter the security settings of the device in any way that will make it fall short of the standards described in this Policy.

We reserve the right, without further notice or permission, to inspect your device and access data and applications on it. To review, copy, disclose, wipe or otherwise use some or all of the company or client data on it, for legitimate reasons, which include enabling us to:

- Audit the device for use of unauthorised applications or software
- Inspect any company or client data stored on the device or on backup or cloud-based storage applications, to prevent misuse of the device and protect company and client data
- Investigate or resolve any security incident or unauthorised use of the IT systems
- Conduct any relevant compliance obligations (including in relation to concerns regarding confidentiality, data protection or privacy)
- Ensure compliance with our rules, standards of conduct and policies (including this policy).

You must co-operate with us to enable such inspection, access and review. A failure to co-operate with us in this way may result in the termination of your engagement and potential legal action.

Technical Support

It is essential that all incidents are reported.

Report any technical support requests by emailing our IT Provider. They will provide initial support to assist in determining if an issue with the device is software or

leading resolutions

hardware related. If the issue is hardware related or relates to software which you have installed, then you will be responsible for resolving it, including any repairs, maintenance or replacements costs and services. If it relates to software or accounts that we have provided, then we will give the necessary support.

Document any information you know while waiting for our IT Provider to respond to an incident. If known, this must include date, time, and the nature of the incident. Any information you can provide will aid in responding in an appropriate manner.

If the incident involves a compromised computer system, or any kind of security breach, suspected or actual, immediately report this to Head Office. The full procedure for this is documented in the **Security Breach Protocol**.

Do not communicate with anyone outside of Leading Resolutions about any details or generalities surrounding any suspected or actual incidents. All communications with law enforcement or the public will be coordinated by the Senior Information Risk Owner, following our Emergency Response Plan.

Selling, Transferring or Replacing a Device

When you intend to sell or transfer your device to anyone else, all company and client data (including e-mails), and any software applications provided by us for business purposes, must be removed from the device by reformatting the hard drive.

End of Policy