ECS EMPLOYEE PUBLIC WORKING POLICY

ECS Policy for Public Working
Dated April 2018

Introduction

We, ECS Resource Group (**'ECS'**), are committed to safeguarding the Personal Data that we gather concerning our prospective, current and former candidates, contractors and clients.
Due to the nature of the business, as is with many other businesses, on occasions members of ECS are required to work when outside of the official office. Therefore this can mean they work within a public space ie. Public transport or any other public domain where there may be a risk of a breach due to a third party seeing, hearing or viewing private information.
This policy is to be enforced in conjunction with ECS Resource Groups data privacy policy.

1. Definitions

This Privacy Policy for Employees shall be referred to as the **"Policy"** and mentions:

- **"Personal data" or "personal information"** - any information relating to an identified or identifiable individual
- **"Data Processing"** - any action or set of actions carried on or using personal data. The gathering, storage, preservation, adjustment, retrieval, disclosure, making available, erasure or destruction of data, or the carrying out of logical and/or arithmetical operations on data; where no automated processing is used, data processing means the processes carried out by our consultants, administrative, and/or any other ECS member of staff for relevant purposes;
- **"Information Systems"** and/or **"CRM Systems"** - any device or group of interconnected devices, one or more of which, conforming to a program, performs automated processing, as well as computer data stored, processed, retrieved or transmitted by them for the purpose of their operation, use, protection or maintenance;
- **"ECS"** or **"ECS Resource Group"** means any person which is directly or indirectly controlled or influenced by ECS Resource Group Ltd.

2. The Application of this Policy

This Policy is evidence that ECS Resource Group is committed to protecting your information. To ensure that at any point an ECS employee has any sensitive information outside of the office, every reasonable step is taken to protect that data.

This Policy applies to any sensitive information regarding our candidates, contractors and clients, whether that be electronic, written or oral.

3. Definition of public working

3.1 As defined by Public Order Act 1936 a "Public place" includes any highway and any other premises or place to which at the material time the public have or are permitted to have access, whether on payment or otherwise ".

3.2 If at any point a member of ECS is working in such a place that there is a risk that any person without relevant permissions could be privy to the sensitive information, then this shall be deemed as a public place.

4.3 If an ECS employee, or anyone affiliated with ECS is required to work in a public place, as previously defined, then they will be subject to the regulations laid out in section 4 of this policy.

4. Ensuring reasonable steps are taken to protect personal data

Any member of ECS who works within a public place, as defined in section 3, will be required to take the appropriate precautions stated in this section.

- Any laptop used must have a protective screen cover as provided by ECS
- Any laptop used must be password protected
- There must be no non-essential data held on that laptop. Any sensitive data held on that laptop must have additional encryption on those files
- When speaking on the phone with clients or candidates, regarding and interview or recruitment process, or any other conversation that contains personal data about any candidate, contractor or client, no sensitive data should be expressly discussed
- No USB devices with sensitive data are to be used in a public place
- Avoid using any printed or written notes or documents whilst working in a public place
- Ensure that no sensitive data is in a physical format whilst working in a public place

5. Data Breach Notification

5.1 All personal data breaches must be reported immediately to the Company's Data Protection Officer or a Director of the Company.

5.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the data protection officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

5.3 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 25.2) to the rights and freedoms of data subjects, the data protection officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

5.4 Data breach notifications shall include the following information:
a) The categories and approximate number of data subjects concerned;
b) The categories and approximate number of personal data records concerned;
c) The name and contact details of the Company's data protection officer (or other contact point where more information can be obtained);
d) The likely consequences of the breach;
e) Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

6. Implementation of Policy

This Policy shall be deemed effective as of 12th April 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

Name: C. EVANS

Position: CEO

Date: 16-4-18

Due for Review by: 1st March 2019

Signature: