Emerald IT Managed Solutions t/a The Emerald Group
Registered Office: 2 Hamilton Terrace, Holly Walk, Leamington, CV34 4LY
Company Registration No: 06876810

Data Protection Policy

Policy information	
Organisation	Emerald IT Managed Solutions t/a The Emerald Group are the Data Controller for the purposes of this policy and hereafter referred to as "the organisation"
Scope of policy	This policy covers all employees of the organisation working in the main HQ, remote working, and working at customer sites It covers the following Data Processors acting on our behalf: The HR Department South Warwickshire, Tracey Hudson Olis & Co, Alan Davies Robert Wood Chartered Accountants, Robert Wood
Policy operational date	1/4/2018
Policy prepared by	Darren Windrum, Managing Director, acting as Data Protection Officer
Date approved by Board	
Policy review date	1/4/2021

Introduction	
Purpose of policy	This policy has been created to ensure the organisation complies with the Data Protection Act 1998 and the new General Data Protection Regulation 2016. It is to ensure the organisation and all employees known and follow best practice to protect clients, colleagues, suppliers, and all other individuals whose data we hold
Types of data	We are the Data Controller for the following data types held by the organisation: • Customer Data e.g. email addresses, domain user names, passwords etc. • Prospect Data e.g. Names, job titles, email addresses • Employee Data e.g. contracts, sick notes, maternity information etc. We hold Customer Data in order to fulfil our contractual obligations We hold Prospect Data with their consent We hold Employee Data for their legitimate interests
Policy statement	We, on behalf of all the individuals whose data we hold, promise to: • Value all data entrusted to us and respect that trust • Go further than the legal requirement and adopt best practice • Always consider and address privacy needs first when planning to use or hold your information in new ways • Be open about how we use your information and who we give it to • Make it easy for you to access and correct your information • Keep the personal information we hold to a minimum and delete it when we no longer need it • Have effective safeguards to ensure your information is securely stored and does not fall into the wrong hands • Provide training for all employees who handle personal information and treat it as a disciplinary matter if they don't look after your information properly • Put appropriate financial and human resource into looking after your information to ensure we live up to our promises • Regularly check that we are living up to our promises and report on our performance
Key risks	The key risks to personal information are: • Ensuring we have appropriate levels of security and access for our Customer Data • Ensuring we have appropriate levels of security and access for our Employee Data • Regularly updating contact information for our customers with checks once a quarter

Responsibilities	
The Board	We have overall responsibility for ensuring that Emerald complies with its legal obligations. Darren Windrum (Director & Chair) Sarah Windrum (Director) Simon Wilks (Director)
Data Protection Officer	Darren Windrum is our appointed Data Protection Officer. His responsibilities are: • Briefing the Board on Data Protection responsibilities • Reviewing Data Protection and related policies • Advising other employees on Data Protection issues • Ensuring that Data Protection induction and training takes place • Notification to the ICO • Handling subject access requests • Approving unusual or controversial disclosures of personal data • Approving contracts with Data Processors
Employees	All employees and interns are required to read, understand, and accept any policies and procedures that relate to the personal data they may handle in the course of their work
Enforcement	Infringements of this policy are dealt with according to our formal HR procedures. All employees are given cyber security training with Sophos, one of our partners and a market-leading expert in internet security

Security	
Scope	Our Data Security measures are detailed below as well as our Business Continuity policy. These are beyond Data Protection and adopted as best practice
Security levels	The greater the consequences of a breach of confidentiality, the tighter the security We have three levels of security for Customer Data: • Level 1: Contact Details • Level 2: User Application Passwords & Financial Data • Level 3: IT Network Passwords e.g. Server, Router etc. We have two levels of security for Employee Data: • Level 1: Contact Details & Training Plans • Level 2: Financial / Health / Performance Reviews We have one level of security for Prospect Data: • Level 1: Contact Details
Security measures	Level 1: Stored digitally in Dynamics CRM and Exchange Contacts. Access for all Emerald employees through password identification Level 2: Stored digitally in the relevant system. Sharepoint (Users), Kashflow & Docuware (Customer Financial), Iris (Employee Financial), Docuware (Employee Health/Performance). Access for restricted Emerald employees only through permission control and password identification Level 3: Stored digitally in RDP Manager. Access for restricted Emerald employees only through permission control and password identification All IT hardware is monitored with anti-virus, anti-spam, anti-malware and ransomware protection through Sophos Central - https://www.sophos.com/en-us/legal/sophos-group-privacy-policy.aspx Our digital data systems are monitored through our own in-house expertise and respective third party hosting: • Docuware: https://start.docuware.com/legal • Microsoft Office 365: https://products.office.com/en-gb/business/office-365-trust-center-privacy • Kashflow: https://www.kashflow.com/privacy-policy/ • Dynamics CRM: https://www.microsoft.com/EN-US/privacystatement/DynamicsCRMOnline/Default.aspx?Search=true&hdrFo=mthdr02 • Iris: https://www.iris.co.uk/company/privacy/ We pro-actively maintain and monitor all IT infrastructure including server, router, and switches and install the latest updates and patches on release. Our router is locked down to only allow access from designated IP addresses to ensure secure VPN access for remote workers Data is not kept in paper form. All paper documents are scanned to the relevant digital system and shredded monthly by Box-It - https://www.boxit.co.uk/company/gdpr/

Business continuity	Our digital systems are replicated to a Tier 3 Data Centre for Business Continuity - https://www.node4.co.uk/colocation/northampton-data-centre/
Specific risks	We complete a starter and leaver form for every change of employee status to ensure appropriate access to data We remote wipe any lost mobile device upon instruction We ensure all hardware containing data is correctly wiped and destroyed We have activated Data Loss Prevention on our hosted email We have a password policy for all users on the network We have network reporting to ensure visibility of threats Level 2 information requested over the phone will be provided with acceptable proof of identity e.g. confirmation of company address, key decision-maker, and another key identifier Level 3 information will never be provided over the phone or by email

Data recording and storage	
Accuracy	Customers: Level 1 data is confirmed for accuracy every 6 months Level 2 data is confirmed for accuracy as relevant during servicing of the contract Level 3 data is confirmed for accuracy at the beginning of the contract and only changed with our consent in accordance to our terms & conditions Employees: It is the employee's responsibility to update us on changes to Level 1 and Level 2 data to ensure accuracy Prospects: Level 1 data is confirmed for accuracy every 6 months
Updating	Level 1 data is updated every 6 months as a minimum. Other data is updated as required.
Storage	All data is stored electronically with access restrictions as detailed in Security Measures
Retention periods	Customer Data is retained throughout the contract period. It is removed 6 months after termination of contract unless otherwise requested. Technical data is kept for archive purposes Employee Data is removed 6 months after termination of employment CVs are removed from our records every 6 months unless given express permission otherwise Prospect Data is retained unless otherwise requested
Archiving	Any records on paper are destroyed monthly by Box-It - https://www.boxit.co.uk/company/gdpr/ All hardware containing digital data is correctly wiped and destroyed Emails are removed or archived every 6 months

Right of Access	
Responsibility	Darren Windrum, as Data Protection Officer, is responsible for subject access requests
Procedure for making request	Subject Access requests should be made in writing to Darren Windrum accessrequest@emerald-group.co.uk You will receive a response and action taken within 30 days in accordance with the ICO guidelines below: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/
Provision for verifying identity	Subject Access requests must provide photo identification and proof of their authority to make the request if they are not known to the organisation
Charging	We reserve the right to seek legal access on complex right of access requests should they arise
Procedure for granting access	Data will be provided in an electronic format We are investigating granting customer access to our main CRM database so they can view and update their own information

Transparency	
Commitment	Emerald are committed to ensuring everyone whose data we hold understands what data we store, how it is processed, why we have it, and who has access to it. We are also committed to ensuring everyone is aware of their rights in relation to this.
Procedure	Our Data Policy is displayed on our website, explained verbally to every Data Subject, and referred to in our Terms & Conditions for Customers and Employee Handbook and Employment Contracts for Employees.
Responsibility	The Directors are responsible for ensuring transparency procedures are followed.

Lawful Basis	
Underlying principles	We hold Customer Data in order to fulfil our contractual obligations We hold Prospect Data with their consent We hold Employee Data for their legitimate interests
Opting out	Customers and Prospects are not able to opt out of their use of their data if they wish us to continue to provide contractual services or employment respectively. Prospect Data is checked every 6 months and able to opt out at any time in between electronically.
Withdrawing consent	All Data Subjects are able to withdraw consent but not retrospectively. If this means we cannot fulfil our contractual obligations, Emerald reserve the right to terminate the agreement in accordance with our Terms & Conditions. If this means we cannot continue with a contract of employment, Emerald reserve the right to terminate the employment in accordance with our Employment Contracts. We reserve the right to consult legal advice in such circumstances.

Employee training & Acceptance of responsibilities	
Induction	All employees have their data handling responsibilities outlined during their induction procedures.
Continuing training	Relevant training is built into our Training Plans for all employees. Updates and non-urgent issues are raised in our Weekly Management Meetings Quarterly Company Meetings.
Procedure for staff signifying acceptance of policy	This Data Protection Policy is included in the Employee Handbook. All employees are required to confirm they have read and understood the policy verbally to the Data Protection Officer

Policy review	
Responsibility	Darren Windrum as Data Protection Officer is responsible for conducting the next review of this policy
Procedure	Third Party providers, the Directors, Finance Manager, IT Operations Manager, Mobile Operations Manager will be consulted in the review
Timing	The review will begin in February 2021