Hitchman Stone Architects Ltd
14 Market Place
Warwick
CV34 4SL

Data Protection Policy

Policy information	
Organisation	Hitchman Stone Architects Ltd is 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 office or remotely It covers the Hitchman Stone Architects Ltd Website It covers the following Data Processors acting on our behalf: Emerald IT Managed Solutions t/a The Emerald Group Bernard Rogers & Co Accountants
Policy operational date	01/05/2018
Policy prepared by	Jeryl Stone, Practice Manager acting in role of Data Protection Officer can be contacted as follows:- Post – Hitchman Stone Architects Ltd 14 Market Place Warwick CV34 4SL Tel: 01926 499456 Email- arch@hitchman-stone.co.uk
Date approved by Proprietor	24th May 2018
Policy review date	01/05/2021

Introduction and Data Protection Principles	
Purpose of policy	This policy has been created to ensure the organisation complies with the Data Protection Act 2018 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 We will comply with data protection law. Personal information that is held will be:- Used lawfully, fairly and in a transparent way Collected only for valid purposes that will be explained and not used in any way that is incompatible with the purposes for which is it intended. Relevant to the purposes involved and limited to those purposes It will be checked for accuracy and kept up to date every six months Will only be kept for as long as necessary for the purposes intended. All data will be kept securely.
Types of data	We are the Data Controller for the following data types held by the organisation: Customer and Project data which we hold to fulfil our contractual obligations and for 12 years post contract Completion/practical completion and any limitation extension of a project years in accordance with professional indemnity requirements. Prospect Data with their consent for 6 months before removing or rechecking for accuracy HR & Payroll Data is held by the Practice Manager and the Accountants only for a maximum of 12 months following cessation of employment of an employee. All HR potential enquiries for employment are stored for 6 months and then destroyed. "**The kind of Information we hold about you** We will collect, store, and use the following categories of personal information about you (where relevant): **Identity Data**: including [personal contact details such as name, title, date of birth, gender, passport, driving licence, national insurance number, photographs, marital status and dependents]. **Contact Data**: including [addresses, telephone and mobile numbers, personal email addresses, next of kin and emergency contact information] **Financial Data**: including [bank account details, payroll records, tax status information, salary, annual leave, pension

	and benefits information]. **Recruitment Data**: recruitment information including [copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process]. **Employment Data**: including [start date, leaving date and your reason for leaving, location of employment or workplace, employment records (including job titles, work history, working hours, holidays, training records and professional memberships), compensation history, performance information, disciplinary and grievance information, [CCTV footage] and other information obtained through electronic means such as information about your use of our information and communications systems, results of HMRC employment status check].” **Data** we hold, needs to be current and accurate for which we will use personal information of employees for the employment history and ongoing working arrangements. We will use employees’ personal information where we need to perform the contract we have entered into with you. **HOW WE USE PARTICULARLY SENSITIVE PERSONAL INFORMATION** "Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data. We may process special categories of personal information in the following circumstances: 1. In limited circumstances, with your explicit written consent. 2. Where we need to carry out our legal obligations or exercise rights in connection with employment. 3. Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our occupational pension scheme. Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.” Website contact details that are input on the “contact us” section of the website are not retained once the information has been actioned. It is then transferred to the in - house contact schedule and reviewed every six months.

Policy statement	The organisation is committed to: • complying with both the law and good practice • respecting individuals' rights • being open and honest with individuals whose data is held • providing training and support for staff who handle personal data, so that they can act confidently and consistently • notifying the Information Commissioner of a potential or actual breach
Key risks	The main risks are: • Ensuring those who work remotely keep data protected especially on mobile devices • Ensuring our on premise document management system (Docuware) is kept secure • Ensuring correct level of security for paper records • Ensuring data is cleared annually after 12 year professional indemnity period • Ensuring our Contacts system is checked for accuracy every 6 months

Responsibilities	
Proprietor and Practice Manager	Stewart Stone (Proprietor) Jeryl Stone (Practice Manager) Have overall responsibility for ensuring the organisation complies with its legal obligations
Data Protection Officer	Jeryl Stone (Practice Manager) is the appointed Data Protection Officer. Her responsibilities are: • Briefing the Board on Data Protection responsibilities • Reviewing Data Protection and related policies • Advising other staff on tricky 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 staff 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 It is important that the personal information held is accurate and current. Employees should notify the Practice Manager if personal information changes during the working relationship with Hitchman Stone Architects Ltd
Enforcement	Any infringement of the Data Protection and associated policies will be dealt with on an individual basis according to our HR procedures

Security	
Scope	Our Data Security measures are detailed below and adopt best practice
Setting security levels	Financial data has a higher level of digital & physical security
IT Security measures	Emerald IT Managed Solutions t/a The Emerald Group provide our IT infrastructure security and provide the services below: Pro-actively monitor anti-virus, anti-spam, anti-malware and ransomware protection on all IT hardware Maintain and support our on-premise digital Document Management System "Docuware" through their own in-house expertise and the third party provider Doctech Host email through Microsoft Office 365 with the latest security updates and protocols 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 Provide data hosting and back-up solutions in a Tier 3 Data Centre - https://www.node4.co.uk/colocation/northampton-data-centre/ Ensure any subject access request requiring data removal is actioned on any back-up data they hold following written instruction from the Data Protection Officer Ensure the organisation's Data Protection Officer is notified if they detect a breach or suspected breach Store all data relating to the servicing of the IT Support contract in accordance with regulations set out by the Data Protection Act 2018 and the General Data Protection Regulation 2016
Other Security Measures	All paper records with financial data are kept in locked filing cabinets Project data is stored on-site for 12 years as required in separate and secure locations within the main building
Specific risks	We complete a starter and leaver form for every change of employee status to ensure appropriate access to data Emerald 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

Data recording and storage	
Accuracy	The accuracy of customer and project data is checked upon initial collection and continually re-confirmed during the project cycle Prospect data is re-checked for accuracy every 6 months
Updating	All data is updated every 6 months as a minimum. Customer and project data is updated more frequently during a project cycle. Upon project completion the data is kept as an archive only for 12 years in accordance with professional indemnity requirements
Storage	Digital records are stored either in hosted email or our on-premise document management database Paper records are stored in a locked filing cabinet if they contain financial data or in a secure on-site location
Retention periods	Customer & Project Data is kept for 12 years in accordance with the requirements for professional indemnity Prospect Data is kept for 6 months
Archiving	Customer & Project Data is archived upon completion Prospect Data is removed after 6 months if accuracy is not re-confirmed. It is removed immediately if consent is removed Emails are continually archived using a hosted solution

Right of Access	
Responsibility	Jeryl Stone (Practice Manager) is responsible for ensuring Right of Access requests are responded to within 30 days
Procedure for making request	Right of access requests must be in writing and email is the preferred method. All employees are required to pass on anything which might be a subject access request to the appropriate person without delay We reserve the right to seek legal access on complex right of access requests should they arise
Provision for verifying identity	Right of access requests verify identity with photo identification where appropriate
Charging	Simple right of access requests are free of charge. We reserve the right to charge a fee to cover administrative costs for any requests that are repetitive or complex
Procedure for granting access	Information will be provided electronically as the preferred method.
Your rights in connection with personal information	Under certain circumstances by law you have the right to:- **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that Hitchman Stone Architects are lawfully processing it. **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected. **Request erasure** of your personal information. This enables you to ask us to delete or remove any personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below) **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes. **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy of the reason for processing it. **Request the transfer** of your personal information to

	another party. If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the Data Protection Officer in writing.

Transparency	
Commitment	The organisation is committed to ensuring individuals are aware that their data is being processed, for what purpose, and how to exercise their rights in relation to data
Procedure	Our Data Protection Policy is displayed on the website, explained verbally to every customer, and referred to in our contract terms
Responsibility	Jeryl Stone (Practice Manager) and Stewart Stone (Proprietor) are responsible for ensuring transparency procedures are followed

Lawful Basis	
Underlying principles	We hold Customer & Project Data to fulfil our contractual obligations We hold Prospect data following a verbal or written enquiry by consent for 6 months
Opting out	We only use Customer & Project Data to fulfil our contractual obligations for completion of the project. We take all the necessary precautions with protecting this data and we must keep it for 12 years for professional indemnity. Upon completion of the project, the data is all archived and only available for access by the Data Protection Officer and Proprietor. Prospect Data is checked every 6 months and given the option to opt out at any time in between by email
Withdrawing consent	The organisation acknowledges that consent, once given, can be withdrawn, but not retrospectively. For the purposes of professional indemnity, the organisation will retain data for the required length of time, even though consent for using it may have been withdrawn

Employee training & Acceptance of responsibilities	
Induction	All employees who have access to any kind of personal data have their responsibilities outlined during their induction procedures
Continuing training	We raise any Data Protection issues during regular team meetings and liaise with our IT provider for any training required on specific issues
Procedure for staff signifying acceptance of policy	All employees have read and accepted the Data Protection Policy by sending email confirmation to the Data Protection Officer

Policy review	
Responsibility	The policy will be reviewed in three years by the Data Protection Officer and Proprietor
Procedure	Emerald Group will be consulted as our third party IT security provider
Timing	The review will begin in April 2021 to ensure it is completed by the appropriate deadline