Data Protection Policy – Simon Scott Electrical

Policy information	
Organisation	Simon Scott Electrical
Scope of policy	This policy applies to the partnership trading as Simon Scott Electrical
Policy operational date	16.05.2018
Policy prepared by	William Scott & Gabrielle Duff
Date approved by Board/ Management Committee	16.05.2018
Policy review date	16.05.2021

Introduction	
Purpose of policy	• complying with the law • following good practice • protecting clients, staff and other individuals • protecting the organisation • transparency
Data Protection Principles	The eight principles of the Data Protection Act 1998 are: 1. Personal data shall be processed fairly and lawfully. 2. Personal data shall be obtained only for one or more specified and lawful purposes. 3. Personal data shall be adequate, relevant and not excessive. 4. Personal data shall be accurate and, where necessary, kept up to date. 5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. 6. Personal data must be processed in accordance with the rights of the individual. 7. Personal data must be kept secure in order to prevent loss or unauthorised disclosure. 8. Personal data shall not be transferred to a country or territory outside the European Economic Area.
Personal data	Data covered by this policy: • Customer data to include: email addresses, phone numbers, home addresses, any access/alarm codes

	• Employee data to include: tax/national insurance details, home addresses, personal email addresses, personal phone numbers, bank details, date of birth, leave records, health records, bonus/profit share schemes, rates of pay/pay increases, emergency contact details, CV's/application forms, exit interviews, references received/supplied, disciplinary/grievance records, appraisals/performance reviews, details of health & safety incidents, training records, employment contracts, work schedules, disabilities, monitoring systems including CCTV, emails & internet, details regarding expenses/company vehicles, attendance & overtime records, details of criminal record including DBS checks & driving offenses, interview notes & assessments, details regarding benefits/pensions

Policy statement	The partnership trading as Simon Scott Electrical Contractors commits to: • Comply with the law and good practice • Apply due diligence in the handling of personal data of both employees and customers • Be open and honest regarding the data protection policies in place • Ensure employees responsible for handling personal data are correctly trained and supported • Respect an individual's rights under the law and respond to requests appropriately in compliance with the law.
Key risks	• information about individuals getting into the wrong hands, through poor security or inappropriate disclosure of information • individuals being harmed through data being inaccurate or insufficient

Responsibilities	
Trustees	William Scott, Simon Scott & Jane Scott
Data Controller	William Scott Responsibilities include: • 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 • Handling subject access requests • Approving unusual or controversial disclosures of personal data • Approving contracts with Data Processors
Specific other staff	Gabrielle Duff
Team/Department managers	N/A
Staff & volunteers	All staff and volunteers should be 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	Data protection offences: • failure of data controllers to notify the Information Commissioner's Office (ICO), or to update their notification entry, as required • obtaining, disclosing, selling or offering to sell personal data without the consent of the data controller, i.e. the organisation processing the information • breaching formal notices issued by the ICO The ICO's action can include: • criminal prosecution for serious breaches • non-criminal enforcement • audits to check organisations are complying • monetary penalties (up to €20,000,000 OR 4% of turnover from previous year, whichever is greater)

Confidentiality	
Scope	Items that come under confidentiality but not Data Protection include: • Information about the organisation • Information about other organisations, since Data Protection only applies to information about individuals • Information which is not recorded, either on paper or electronically • Information held on paper, but in a sufficiently unstructured way that it does not meet the definition of a "relevant filing system" in the Data Protection Act
Understanding of confidentiality	Any sharing of confidential information is to be dealt with on a case-by-case basis, as a rule of thumb information is not to be shared outside of the company and any sharing of information within the company will be on a "need to know" basis, to be approved by the nominated Data Controller.
Communication with Data Subjects	The subject of any confidential data will be notified, and permission sought in writing, before any data is shared, the only exception being if data is requested by court order.
Communication with staff	Staff are to be appropriately trained in Data Protection upon induction with refresher training conducted as appropriate. Staff contracts are to detail relevant sharing under Data Protection.
Authorisation for disclosures not directly related to the reason why data is held	Instigated by or in the interests of the data subject: • Requests to be made in writing to the Data Controller • Data subject to be notified and to authorise disclosures of this kind in writing • Records to be maintained In the course of official investigations: • Data Controller to authorise any disclosures • Evaluation of disclosure to be made on a case-by-case basis • Data Controller to decide if data subject needs to be notified on a case-by-case basis

Security	
Scope	All items that come under the scope of confidentially should have an appropriate security measure in place to ensure no breaches of data are allowed to occur.
Setting security levels	• Medium level: Customer records, as no bank details, tax records etc are held customer records should be stored securely but the data held is not high risk • High level: Employee records, as bank records, tax details, national insurance numbers etc are held this data is high risk
Security measures	• Medium level: Data is to be stored on password protected systems and secure cabinets for any hard copies, CCTV is in place at the location of the storage of hard copies. • High level: Data is to be stored securely in encrypted files and on password protected software, hard copies are stored in a locked cabinet, access to data is limited to Data Controller and specific other staff named in this policy, CCTV is in place at the location of storage.
Business continuity	Data is stored on a cloud accounting system (namely Sage One) and protected by said systems encryption and security as well as password protection. Data is also stored on Microsoft SharePoint, itself securely encrypted and password protected and only accessible by the DPO and specific other staff named in this policy. Hard copies of data are securely stored in locking cabinets on premises under CCTV monitoring. Data is shared within the business on a "need to know" basis only.
Specific risks	• Working away from the business premises: data handled when working off premises is on a "need to know" basis only and is not to be shared beyond those to whom data is expressly given i.e. employees given customers' addresses/contact details to attend a job • Working from home: any data taken off premises to be worked on at home or other location should first be authorised for removal from the premises by the DPO and then be securely kept by the employee authorised, no copies of data are to be made away from the premises without authorisation of the DPO • When dealing with data requests over the phone/email firstly establish if the requester is authorised to receive said information, check with the DPO if the request is genuine. All requests must be made in writing (either via letter or email). • Staff personal contact details are not to be shared,

	however each employee is given a work phone where applicable and said phone number may be given if the request is deemed to be appropriate. Personal contact details are never to be shared with third parties.

Data recording and storage	
Accuracy	When taking customer details over the phone ask the customer to repeat number and email back to you to ensure you hold the correct details. Avoid repeating details back to the customer.
Updating	When customers' contact the business to request new works ask them to confirm any contact details held.
Storage	Data is held on: Sage One – cloud accounting software, Microsoft SharePoint – Cloud storage and hard copies are securely stored in lockable cabinets.
Retention periods	See page 15
Archiving	See page 15

Subject access	
Responsibility	As Data Controller, William Scott will ensure these policies and the law are adhered to and that subject access requests are handled within the legal time limit of 30 days.
Procedure for making request	Subject access requests are to be made in writing to William Scott either in writing to: Unit C The Old Laundry Trading Estate Sea Road North Bridport Dorset DT6 3BD UK Or via email to: info@simonscottelectrical.co.uk
Provision for verifying identity	Before granting subject access requests appropriate measures must be taken to ensure the identity of the person requesting the information. The following methods can be used: • Ask the requester to confirm via telephone some of the contact details held • Ask the requester to send a copy of a passport/driving license
Charging	There is a £5.00 admin fee in place for such requests.
Procedure for granting access	Should access be granted a hard copy of the data authorised should be securely given to the requester.

Transparency	
Commitment	Simon Scott Electrical commits to ensuring data subjects have access to what types of data are held, the purpose for it being held, the length of time it will be held and their right to request access to any information held regarding themselves.
Procedure	Data subjects will be informed, where necessary, in the following ways: • Employee handbooks • The business' website
Responsibility	Responsibility falls on the Data Controller to ensure transparency is maintained regarding data collected and held.

Consent	
Underlying principles	• We have made the request for consent prominent and separate from our terms and conditions. • We ask people to positively opt in. • We don't use pre-ticked boxes or any other type of default consent. • We use clear, plain language that is easy to understand. • We specify why we want the data and what we're going to do with it. • We give separate distinct ('granular') options to consent separately to different purposes and types of processing. • We name our organisation and any third-party controllers who will be relying on the consent. • We tell individuals they can withdraw their consent. • We ensure that individuals can refuse to consent without detriment. • We avoid making consent a precondition of a service
Forms of consent	Consent can be given either; verbally, in writing or via an opt in form.
Opting out	Any marketing mailers have a simple to use opt out option.
Withdrawing consent	When possible if consent is withdrawn data will be destroyed in good time. However, exceptions must be made for accounting purposes, tax records and legal liabilities in which case a note will be made of the withdrawal of consent and once it is possible to dispose of said data it will be destroyed as requested. Data subjects will be notified in either case as to when the withdrawal of data will be completed.

Direct marketing	
Underlying principles	• We use opt-in boxes • We specify methods of communication (e.g. by email, text, phone, recorded call, post) • We ask for consent to pass details to third parties for marketing and name those third parties • We record when and how we got consent, and exactly what it covers
Opting out	• We only text or email with opt-in consent (unless contacting previous customers about our own similar products, and we offered them an opt-out when they gave their details) • We offer an opt-out (by reply or unsubscribe link) • We keep a list of anyone who opts out • We screen against our opt-out list
Sharing lists	We do not share lists of data with any third parties.

Staff training & acceptance of responsibilities	
Documentation	The employee handbook includes a section on data protection, an employee notice is also given to new starters and signed on commencement of employment.
Other related policies	• The employee handbook • Employee data protection notice
Induction	All staff who have access to any kind of personal data should have their responsibilities outlined during their induction procedures.
Continuing training	Refresher training is given as appropriate.
Procedure for staff signifying acceptance of policy	Staff are to read and sign an employee data protection notice on commencement of employment as well as their contract the terms of which, including data protection, are outlined in the employee handbook.

Policy review	
Responsibility	It falls to the named Data Controller to conduct the next review of this policy on 16.05.21
Procedure	The partners of Simon Scott Electrical will approve any amendments made to the policy on review.
Timing	This policy will be reviewed every three years. The next review is due on 16.05.21

Description of Data Held	Whose Data is Held	Length of Time Data is Held	Reason Data is Held	Type of Records	Disposal Process	Data Security Measures
HR Files	Current Employees Former Employees	Indefinitely	For payroll purposes, tax records, due diligence, legal compliance	Digital & Hard Copy	The disposal of data is to be recorded and witnessed by one of the partners. Digital records are to be wiped. Hard copies are to be shredded and securely disposed of.	Digital copies: Files password protected and encrypted Hard copies: Kept in locked cabinet in premises with CCTV protection
Names	Current Employees Former Employees Customers Job Applicants	Indefinitely	For work records, contacting regarding works/accounting/payroll, tax records, accounting, payroll	Digital & Hard Copy	The disposal of data is to be recorded and witnessed by one of the partners. Digital records are to be wiped. Hard copies are to be shredded and securely disposed of.	Digital copies: Files password protected and encrypted Hard copies: Kept in locked cabinet in premises with CCTV protection
Date of Birth	Current Employees Former Employees	5 Years from end of employment	Payroll purposes, tax records, legal compliance	Digital & Hard Copy	The disposal of data is to be recorded and witnessed by one of the partners. Digital records are to be wiped. Hard copies are to be shredded and securely disposed of.	Digital copies: Files password protected and encrypted Hard copies: Kept in locked cabinet in premises with CCTV protection
Contact Details	Current Employees Former Employees Customers Job Applicants	Indefinitely	For contacting regarding accounting, works, payroll, employment, tax records	Digital & Hard Copy	The disposal of data is to be recorded and witnessed by one of the partners. Digital records are to be wiped. Hard copies are to be shredded and securely disposed of.	Digital copies: Files password protected and encrypted Hard copies: Kept in locked cabinet in premises with CCTV protection

Application Forms & CVs	Current Employees Former Employees Job Applicants	5 Years from end of employment	Due diligence, equal opportunities, employment opportunities,	Digital & Hard Copy	The disposal of data is to be recorded and witnessed by one of the partners. Digital records are to be wiped. Hard copies are to be shredded and securely disposed of.	Digital copies: Files password protected and encrypted Hard copies: Kept in locked cabinet in premises with CCTV protection
Interview Notes & Assessments	Current Employees Former Employees Job Applicants	5 Years from end of employment	For company records, due diligence, future employment opportunities, compliance with the Equal Opportunities act	Digital & Hard Copy	The disposal of data is to be recorded and witnessed by one of the partners. Digital records are to be wiped. Hard copies are to be shredded and securely disposed of.	Digital copies: Files password protected and encrypted Hard copies: Kept in locked cabinet in premises with CCTV protection
Details of Criminal Records including DBS checks & Driving Offenses	Current Employees Former Employees	5 Years from end of employment	For due diligence, protection of vulnerable people, insurance purposes, works completed in premises housing vulnerable people e.g. schools or care homes	Digital & Hard Copy	The disposal of data is to be recorded and witnessed by one of the partners. Digital records are to be wiped. Hard copies are to be shredded and securely disposed of.	Digital copies: Files password protected and encrypted Hard copies: Kept in locked cabinet in premises with CCTV protection
Annual Leave Sick Leave & other types of leave	Current Employees Former Employees	5 Years from end of employment	For legal compliance, tax records, accounting, payroll purposes	Digital & Hard Copy	The disposal of data is to be recorded and witnessed by one of the partners. Digital records are to be wiped. Hard copies are to be shredded and securely disposed of.	Digital copies: Files password protected and encrypted Hard copies: Kept in locked cabinet in premises with CCTV protection
Records regarding pay & pay increases, bonuses, commission & profit share	Current Employees Former Employees	6 Years from end of employment	For payroll purposes, tax records, due diligence, legal compliance	Digital & Hard Copy	The disposal of data is to be recorded and witnessed by one of the partners. Digital records are to be wiped. Hard copies are to be shredded and securely disposed of.	Digital copies: Files password protected and encrypted Hard copies: Kept in locked cabinet in premises with CCTV protection

Monitoring systems including CCTV, internet, email	Current Employees Former Employees Customers Job Applicants	5 Years	For security, records of works, accounting purposes	Digital	The disposal of data is to be recorded and witnessed by one of the partners. Digital records are to be wiped. Hard copies are to be shredded and securely disposed of.	Digital copies: Files password protected and encrypted Hard copies: Kept in locked cabinet in premises with CCTV protection
National Security Numbers/Records & Income Tax Information	Current Employees Former Employees	5 Years from end of employment	For tax records, payroll purposes, accounting history	Digital & Hard Copy	The disposal of data is to be recorded and witnessed by one of the partners. Digital records are to be wiped. Hard copies are to be shredded and securely disposed of.	Digital copies: Files password protected and encrypted Hard copies: Kept in locked cabinet in premises with CCTV protection
Emergency Contact Details	Current Employees Former Employees	5 Years from end of employment	For emergency situations	Digital & Hard Copy	The disposal of data is to be recorded and witnessed by one of the partners. Digital records are to be wiped. Hard copies are to be shredded and securely disposed of.	Digital copies: Files password protected and encrypted Hard copies: Kept in locked cabinet in premises with CCTV protection
References - received & supplied	Current Employees Former Employees Job Applicants	5 Years from end of employment	For due diligence, protection of vulnerable people, insurance purposes, works completed in premises housing vulnerable people e.g. schools or care homes	Digital & Hard Copy	The disposal of data is to be recorded and witnessed by one of the partners. Digital records are to be wiped. Hard copies are to be shredded and securely disposed of.	Digital copies: Files password protected and encrypted Hard copies: Kept in locked cabinet in premises with CCTV protection
Health information (reasons for absence, return to work meetings, GP notes, occupational health advice, details of disabilities that may require reasonable work adjustments)	Current Employees Former Employees	40 Years from end of employment	For legal compliance, tax records, accounting, payroll purposes, compliance with Disability Discrimination Act	Digital & Hard Copy	The disposal of data is to be recorded and witnessed by one of the partners. Digital records are to be wiped. Hard copies are to be shredded and securely disposed of.	Digital copies: Files password protected and encrypted Hard copies: Kept in locked cabinet in premises with CCTV protection

Details regarding expenses & company vehicles	Current Employees Former Employees	5 Years from end of employment	For accounting purposes, payroll, tax records	Digital & Hard Copy	The disposal of data is to be recorded and witnessed by one of the partners. Digital records are to be wiped. Hard copies are to be shredded and securely disposed of.	Digital copies: Files password protected and encrypted Hard copies: Kept in locked cabinet in premises with CCTV protection
Bank account details	Current Employees Former Employees	5 Years from end of employment	For payroll purposes	Digital & Hard Copy	The disposal of data is to be recorded and witnessed by one of the partners. Digital records are to be wiped. Hard copies are to be shredded and securely disposed of.	Digital copies: Files password protected and encrypted Hard copies: Kept in locked cabinet in premises with CCTV protection
Employment contracts	Current Employees Former Employees	5 Years from end of employment	For accounting purposes, tax records, payroll purposes, legal compliance	Digital & Hard Copy	The disposal of data is to be recorded and witnessed by one of the partners. Digital records are to be wiped. Hard copies are to be shredded and securely disposed of.	Digital copies: Files password protected and encrypted Hard copies: Kept in locked cabinet in premises with CCTV protection
Details of nationality & entitlement to work in the UK	Current Employees Former Employees	5 Years from end of employment	Compliance with The Right to Work in The UK Law	Digital & Hard Copy	The disposal of data is to be recorded and witnessed by one of the partners. Digital records are to be wiped. Hard copies are to be shredded and securely disposed of.	Digital copies: Files password protected and encrypted Hard copies: Kept in locked cabinet in premises with CCTV protection
Work schedules	Current Employees Former Employees	5 Years from end of employment	Payroll purposes, tax records, legal compliance with Working Hours, billing purposed	Digital & Hard Copy	The disposal of data is to be recorded and witnessed by one of the partners. Digital records are to be wiped. Hard copies are to be shredded and securely disposed of.	Digital copies: Files password protected and encrypted Hard copies: Kept in locked cabinet in premises with CCTV protection

Attendance & overtime records	Current Employees Former Employees	5 Years from end of employment	Payroll purposes, tax records, legal compliance with Working Hours	Digital & Hard Copy	The disposal of data is to be recorded and witnessed by one of the partners. Digital records are to be wiped. Hard copies are to be shredded and securely disposed of.	Digital copies: Files password protected and encrypted Hard copies: Kept in locked cabinet in premises with CCTV protection
Disciplinary or grievance investigations, meeting records & warnings	Current Employees Former Employees	6 Years from end of employment	Legal compliance, payroll purposes, accounting purposes	Digital & Hard Copy	The disposal of data is to be recorded and witnessed by one of the partners. Digital records are to be wiped. Hard copies are to be shredded and securely disposed of.	Digital copies: Files password protected and encrypted Hard copies: Kept in locked cabinet in premises with CCTV protection
Records of health & safety incidents	Current Employees Former Employees	40 years	Legal compliance, insurance	Digital & Hard Copy	The disposal of data is to be recorded and witnessed by one of the partners. Digital records are to be wiped. Hard copies are to be shredded and securely disposed of.	Digital copies: Files password protected and encrypted Hard copies: Kept in locked cabinet in premises with CCTV protection
Appraisal & other performance reviews	Current Employees Former Employees	5 Years from end of employment	Payroll, legal compliance, due diligence	Digital & Hard Copy	The disposal of data is to be recorded and witnessed by one of the partners. Digital records are to be wiped. Hard copies are to be shredded and securely disposed of.	Digital copies: Files password protected and encrypted Hard copies: Kept in locked cabinet in premises with CCTV protection
Details regarding benefits & pensions	Current Employees Former Employees	6 Years from the of the scheme year in which the event took place	Payroll, legal compliance, due diligence, tax records, accounting purposes	Digital & Hard Copy	The disposal of data is to be recorded and witnessed by one of the partners. Digital records are to be wiped. Hard copies are to be shredded and securely disposed of.	Digital copies: Files password protected and encrypted Hard copies: Kept in locked cabinet in premises with CCTV protection

Exit interviews	Former Employees	5 Years from end of employment	Due diligence, equal opportunities,	Digital & Hard Copy	The disposal of data is to be recorded and witnessed by one of the partners. Digital records are to be wiped. Hard copies are to be shredded and securely disposed of.	Digital copies: Files password protected and encrypted Hard copies: Kept in locked cabinet in premises with CCTV protection
Emails & texts about staff	Current Employees Former Employees	5 Years from end of employment	Payroll, legal compliance, due diligence, equal opportunities, disability discrimination act	Digital	The disposal of data is to be recorded and witnessed by one of the partners. Digital records are to be wiped. disposed of.	Digital copies: Files password protected and encrypted