SIMPSON ARBORICULTURE LTD.
TREE SURGERY · FORESTRY · FIREWOOD

31

Simpson Arboriculture Ltd

Privacy (GDPR)

Policy Section Number	31
Date Ratified	01/11/2025
Version Number	1
Next Review Date	01/11/2026
Related Policies and Guidance Documents	All Policies
Related Regulations	The Data Protection Act 1998 GDPR 2018
Annexes and Supplementary Info	None
Responsible Person	Will Simpson & Kate Simpson
Responsible Person Signature	

1.0 Policy Statement

1.1 This is Simpson Arboriculture Ltd's Policy and statement of the purposes for which the Company hold personal data about the Company's employees, other businesses and others who work for us in accordance with the Data Protections Act 1998 ("the Act") and the European General Data Protection Regulation ("the Regulation") which came into force May 2018.

2.0 Employee Data

2.1 Simpson Arboriculture Ltd will collect, hold, and process information consisting of personal data including sensitive personal data (see below) about all the Company's employees, applicants for employment, self-employed contractors, agency workers and others who work for us, who are referred to in the Act as "data subjects".

2.2 Personal data relating to Data Subjects includes anything that allows that Data Subject to be identified and could include (but is not limited to):

2.2.1 A name

2.2.2 Postal Address

2.2.3 Email Address

2.2.4 An Internet Protocol ("IP" Address)

2.2.5 Sort Code or Bank Account information

2.2.6 A copy of a Passport, Driving Licence or photo ID

2.2.7 A photograph

2.2.8 An audio recording

2.2.9 A video recording

2.3 The Company hold information about data subjects solely for administrative and personnel management purposes. This includes but it is not limited to recruitment, appraisals, performance, promotion, training, career development, pay and remuneration, pension and insurance and other deductions from pay health and safety discipline and grievances, marketing products and services to the Company's workers and the review of the Company's Human Resources policies.

3.0 Sensitive Data

3.1 The Act defines "Sensitive personal data" as personal data consisting of information as to racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, membership of a trade union, physical or mental health condition, sexual life, the commission or alleged commission of any offence or any proceedings for any offence committed or alleged to have been committed, including the disposal of such proceedings or the sentence of any court in such proceedings.

3.2 The purpose for which the Company hold sensitive personal data about data subjects is for use solely for equal opportunities monitoring or for the provision of specific services to individuals.

3.3 This includes but is not limited to: assessing suitability and fitness for work, administering sick pay and sick leave, absence control, maternity leave and pay, safe environment and complying with the Company's obligations under the relevant legislation.

4.0 Retention of Data

4.1 The purpose for which the Company hold any information about data subjects after the end of employment is solely for any residual employment related matters including but not limited to the provision of job references, processing applications for re-employment, matters relating to retirement benefits and allowing us to fulfil contractual or statutory obligations.

5.0 Statutory Purposes

5.1 In addition to the above purposes, the Company may collect, hold, and process data including sensitive personal data if it is necessary to do so for compliance with any statutory duty with which the Company are required to comply.

6.0 Third Parties

6.1 If necessary, the Company may transfer personal data to insurers, bankers, legal, medical, and other professional advisers, administrators of the Company's pension scheme or your own pension provider and other companies to which the Company have contracted work relating to any of the above purposes for which the personal data are to be used.

6.2 Data may be disclosed to others at an employee's own request.

6.3 Data will only be disclosed to a third party provided express consent is obtained from the employee for each specific discreet purpose.

7.0 Electronic Communications

7.1 The Company monitor electronic communications by employees, including websites, to ensure that these systems are used in accordance with the Company's email, internet, and telephone policy.

7.2 All monitoring of electronic communications is carried out in accordance with the relevant legal and regulatory standards.

8.0 Good Practice

8.1 The Data Protection Act sets out eight enforceable principles of good practice to which the Company will make all reasonable efforts to adhere. These principles are that the data must be:

8.1.1 Fairly and lawfully processed.

8.1.2 Processed for limited purposes and not in any manner incompatible with those purposes.

8.1.3 Adequate, relevant, and not excessive

8.1.4 Accurate

8.1.5 Not kept for longer than is necessary.

8.1.6 Processed in accordance with individuals' rights.

8.1.7 Secure

8.1.8 Not transferred to countries outside the EU without adequate protection.

9.0 Subject Access Rights

9.1 All individuals who are the subject of personal data held by the Company are entitled to:

9.1.1 Ask what information the Company holds about them and why.

9.1.2 Ask how to gain access to it.

9.1.3 Be informed how to keep it up to date.

9.1.4 Be informed how the Company is meeting its data protection obligations.

9.1.5 Have the right to request that all their personal data held by the Company be deleted under the “Right to be forgotten” within the Regulation.

9.2 If an individual contacts the Company requesting this information, this is called a subject access request.

9.3 Subject access requests from individuals should be made by email, addressed to the data controller, please see your line manager for who is the data controller within the company. The Data controller can supply a standard request form, although individuals do not have to use this.

9.4 Individuals maybe charged to attain this information per subject access request. The data controller will aim to provide the relevant data within 14 days. The data controller will always verify the identity of anyone making a subject access request before handing over any information.

9.5 Any individual requesting that their data be deleted under the “Right to be Forgotten” Regulation must have their request acknowledged in writing. All relevant data across all files, databases and systems must be deleted, including any references where applicable, to an individual who has been mentioned on any social media accounts, websites, or blogs under the control of the Company. This should also include, where applicable, any photographs, audio recording, video recordings or any other data that could allow that individual to be identified. If for any reason it is not possible or impractical to delete any data relating to the individual the Company must account for any records that will continue to be maintained.

10.0 References

10.1 Providing a reference involves the disclosure of personal data of the individual who is the subject of the reference. To ensure protection of the Company’s employees’ data no reference (whether to prospective employers or other institutions) should be given on behalf of the Company without prior authorisation. All reference requests are usually dealt with through the HR Representative, in the first instance.

10.2 This Policy does not prevent any employee giving a reference in a personal capacity, but employees should make clear that such references are personal and not on behalf of the Company and, if the reference is given on paper. It is the Company’s policy to provide a written standard reference which outlines an employee’s main particulars.

11.0 Employee Obligations

11.1 During the Company’s business, the Company collect and process personal information, including that relating to employees, contacts, members, potential customers, and suppliers to which you may have access in the course of your employment. It is the Company’s policy to ensure compliance by the Company’s employees with the Act. The Company reserve the right to implement the Disciplinary Policy against anyone who fails to comply with the procedures set out below.

11.2 This section of the Policy provides guidance to all staff on their obligations in respect of accessing, holding or using personal information during their employment, such as member and contact information and information relating to other members of staff. It applies to all employees.

11.3 The Company must also comply with the terms of the Act in relation to its marketing activities, Further advice and guidance in this respect may be obtained from your Manager.

11.4 The Act requires that all personal information be kept confidential and secure.

11.4.1 Therefore:

11.4.1.1 You must observe all instructions or directions you are given from the Company or your Manager in respect of confidentiality and security or information.

11.4.1.2 You must comply with all security obligations under the Company's Internet, Email and Telephone Policy.

11.4.1.3 You must comply with all confidentiality obligations contained within your employment contract.

11.4.1.4 You must keep workstations locked when away from desks and keep any documentation containing personal information out of sight overnight, not left out on desks.

11.4.1.5 PCs should be protected by strong passwords that are changed regularly and never shared between employees.

11.4.1.6 If data is stored on removable media (like a CD, or DVD or USB device), these should be locked away securely when not being used.

11.4.1.7 Any personal data stored on removable media should be encrypted using a secure encryption tool that requires a unique password to retrieve the data.

11.4.1.8 Data should only be stored on designated drives and servers and should only be uploaded to an approved cloud computing services, Personal data should on no account be stored on freely available cloud platforms such as Dropbox or Google Drive.

11.4.1.9 Personal data should on no account be stored or transmitted on any social media platforms such as WhatsApp, Facebook, or LinkedIn.

11.4.1.10 Servers containing personal data should be sited in a secure location, away from general office space.

11.4.1.11 Data should be backed up frequently. Those backups should be tested regularly, at least every 6 months.

11.4.1.12 Data should never be saved directly to personal laptops or other mobile devices like tablets or smart phones.

11.4.1.13 All data that is stored on servers should be protected by approved security software and a firewall when working with personal data, employees should ensure the screens of their computers are always locked when left unattended.

11.4.1.14 Employees should not save copies of personal data on their own computers.

11.4.1.15 Personal data should not be taken off site unless held on a secure device and prior permission is given by the Line Manager, for example when working from home.

11.4.1.16 Any employee given permission to work from home using personal data should ensure that personal data is not used on any device that could be overlooked in a public space while being worked on such as

a train or café. Personal data should not be worked on using a device that is connected to an unknown or unsecure public Wi-Fi network.

11.4.1.17 Any work on personal data in the home environment where the employee needs to be online should only take place on a home Wi-Fi or cable internet connection onto a home network is limited to the employee and immediate close family.

11.4.1.18 Any personal data that is used while working from home that is in a hardcopy format that needs to be destroyed must be securely shredded or returned for destruction in confidential waste and on no account, should be destroyed with general household waste.

11.4.1.19 All terminals, laptops or devices used to view personal data should have a minimum level of antivirus and anti-malware software installed.

11.4.1.20 When working out of the office of from home, be aware of where devices are being charged from. Some public charging points could be compromised or could allow for the data on devices to be accessed by a third-party during charging in a process known as “juice jacking”.

11.4.1.21 You must ensure that the operating systems on all IT hardware including laptops and tablets are fully up to date. Obsolete operating systems or web browsers that are no longer supported and not receiving updates or patches will be highly vulnerable to exploitation in a cyber-attack.

11.4.1.22 You must inform us of any changes to your personal details to enable us to comply with the Act and to aid the smooth running of the business.

11.4.1.23 You must inform us of any changes to your personal details to enable us to comply with the Act and to aid the smooth running of the business.

11.4.1.24 You must keep all lockable cabinets and drawers in which personal information is stored locked when not in use.

11.4.1.25 Any hard copy records containing personal data should be kept in files that are clearly marked “Protect: Personal Data” to ensure that all staff are able to identify a file quickly and easily as containing personal data and to treat that data in accordance with the governance procedures outlined in this policy.

11.4.1.26 Any hard copy personal data to be sent via the Post, DX or other means should be sent in a secure and trackable manner. This should mean all post containing personal data is sent via Special Delivery.

11.5 Information held must be accurate, relevant, and not excessive. If you need to hold or collect personal information you must therefore:

11.5.1 Ensure that all documents containing personal information are up to date and held for no longer than is necessary. You should be aware that what constitutes “no longer than necessary” will vary and takes into consideration the type of information and the purpose for which it is being solved.

11.5.2 Ensure that all documentation or other materials no longer required containing personal information are disposed of via a secure confidential waste method/shredder.

11.5.3 Ensure that the content of personal information held is objective.

11.5.4 Ensure that the information you hold may be disclosable/disclosed to the individual concerned.

11.6 Staff need to ensure that only the "authorised processing of information" takes place. In practice this means that:

11.6.1 Information held and used must be required by you in the information in the course of your employment,

11.6.2 You must not access, gather, or hold information which you do not genuinely need to carry out your job.

11.6.3 Access to personal information should be refused to individuals both internally and externally (without the consent of the individual) unless these individuals are authorised to access or process such information. Please see membership data allowance clause below.

11.6.4 Expect in certain limited circumstances, it is a criminal offence to obtain or disclose personal data or the information contained in personal data or the information contained in personal data or to procure the disclosure of the information contained in personal data to another person without the consent of the person responsible for the Company's compliance with the Act. This means that:

11.6.5 You may be committing a criminal offence if you do not process data in an authorised manner, whether you do so deliberately or because you have not taken sufficient care.

11.6.6 It is extremely important that you comply with the terms of this Policy and with any further instructions or directions the Company or your Manager give you.

11.6.7 If you have any doubts or queries concerning your access to, or use of, personal data in the course of your employment, you should seek guidance form the HR Representative.

11.6.8 Duties and areas of responsibility shall be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation's assets. For example, in terms of Business

11.7 Support work. The three areas are "Identification", "Audit" and "Claim". No one person can undertake two adjourning tasks.

12.0 Notices

12.1 Where personal data is to be provided by a Data Subject, the Regulations require that the Data Subject be made aware of following:

12.1.1 The legal basis for processing the data.

12.1.2 The period for which the data shall be retained,

12.1.3 That the individual has a right to complain to the UK Data Protection Regulator, the Information Commissioner's Office ("ICO").

12.1.4 Whether there is a statutory or contractual requirement to provide the data.

12.1.5 What would be the consequences for the Data Subject of not providing the data.

13.0 Consent

13.1 Where required under the Act and the Regulation, consent must be obtained from the data subject. Consent must be in writing (hardcopy or email) and must be expressly provided for the purpose for which the data is being used. Consent must be:

13.1.1 Freely given (not under inducement, duress or otherwise pressured from the data subject).

13.1.2 Specific ("Bulk" consent got multiple purposes is not sufficient. Specific consent is required for a specific purpose).

13.1.3 Informed (a tick box with no explanation as to how the data is to be used is not sufficient, enough information must be provided to the data subject so that they may make an informed decision.

13.1.4 Unambiguous (plain English should be used in the language that obtains consent and there should be no additional or implied purpose that could be construed from the provision of the consent).

13.2 The data subject must have the right to withdraw their consent at any time.

13.3 Adequate records must be maintained where consent has been provided with a full audit trail that can be evidenced. Where children are below 13 years of age, parental consent for the processing of their data must be obtained prior to processing being carried out.

14.0 Contact for Further Advice on Data Protection

14.1 The Company's Managing Director has overall responsibility for the Company's compliance with the Act, including registration and regular monitoring.

14.2 The Company delegate compliance on a practical level insofar as customer information is concerned, and compliance on all employee data as appropriate.

14.3 The Managing Director is the designed "Data Controller" and registered with the Information Commissioner's Office (ICO). The Data Protection Officer is the Company Managing Director. They are supported in ensuring compliance with this policy across the organisation by The Managing Director.