MALLINSON PLUMBING AND HEATING
DATA PROTECTION POLICY

1. The General Data Protection Regulation (GDPR) applied from 25th May 2018. This policy is effective from 1st July 2018 and applies to all directors, employees, volunteers, and those working on a temporary basis or through an agency (all together referred to as “employees”) for F. & R. Mallinson Limited (“company”).

2. This policy must be read and applies in conjunction with the HR Policy (“Policies”).

3. The company’s Data Compliance Manager is Phillip Mallinson. The Deputy Data Compliance Manager is Linda Mallinson. The company is registered with the Information Commissioner’s Office with registration number ZA444299.

4. The Policies together document the company’s obligations under the GDPR and how the company intends to comply with these obligations. The company will document so far as is reasonably practicable decisions made in relation to the processing of any data.

5. Personal Data is defined by the GDPR as any information relating to an identified or identifiable natural person (‘data subject’), an identifiable natural person is one who can be identified, whether directly or indirectly, by reference to the person’s name, an identification number, location data, an online identifier (email address) or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

6. Any reference in this policy to data means both Personal Data and Special Category Data. The company processes Special Category Data relating to its employees. This is set out in further detail in the company’s HR Policy.

7. The processing of data means any operation or set of operations which is performed (whether or not by automated means), such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. As such, wherever the company holds data in any format this amounts to processing.

Mallinson
Plumbing & Heating

8. The company will comply with its obligations under Article 5 of the GDPR to ensure that any data:

- is processed lawfully, fairly and in a transparent manner
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is not
compatible with these purposes
- will be adequate, relevant and limited to what is necessary in relation to the purpose which the Firms hold the data
- accurate and kept up to date and erased or rectified without delay
- kept in a form which permits identification of the individual for no longer that is necessary for the purposes for which the data is obtained and processed
- is processed in a manner which ensures security of the personal data (and which includes unauthorised or unlawful processing, accidental loss, destruction or damage.

Lawful bases for processing

9. For the company to lawfully process data it must comply with Article 6 of the GDPR which lists the grounds upon which the data can be lawfully processed.

10. The company has conducted an audit into the data it holds and has determined that it holds the following data and the lawful basis for processing that data to be as follows:

(i) The company obtains data from its customers when they enter into a contract with the company to provide heating or plumbing services. The company processes the data for the purpose of undertaking the contract. This data includes the customer's name, home address, the address of any premises where the company undertakes work, email addresses, telephone number, payment details and details of the work that the company undertake. The company considers this is necessary to undertake the work and perform the contract.
(ii) After the company has completed the contract, it will retain all of the data except for the payment details or bank information of its customers. The company considers that this is necessary in the legitimate interests of its business and also in the legitimate interests of its customers as it maintains records of the work done and particularly when servicing of customer's systems is due or warranties expire in order that the company may contact them to inform them.
(iii) The company obtains and retains data of those who visit its website. The cookies on the company's website retains information about the identifier of the website users and such other computer data. This is retained as it is necessary in the legitimate interests of the company to assist with analytical purposes, and monitor and where necessary develop and improve the website as well as in the legitimate

interests of the website visitors themselves to facilitate use of the website and is set out in the Cookie policies on the website.
(iv) The company holds and processes data relating to employees. There are different lawful bases for holding this data and in this respect please see the company's HR Policy.

11. The company has considered and determined that the processing of data under paragraph 10 (i), (ii) and (iii) is necessary for the lawful bases stated.

12. Data processed under paragraph 10(i) and (ii) may be held both electronically on the company's SAGE computer program and on paper.

13. The company has sent a copy of its Privacy Notice to all existing customers whose data is held in the legitimate interests of the business / customer and informed them that if they wish to object to the processing they may do so and how to do so.

14. The company will send a copy of its privacy notice to all new customers who enter into contracts with it. In addition, a copy of the privacy notice will be put on the company's website.
15. In the event that the company should determine to seek consent of consumers (and maybe business / trade account customers) to hold any data for marketing purposes the company shall obtain the specific consent of the individual. The company recognises in this instance that the consent must be freely given, for a specified purpose /s and the individual must be informed and specifically agree and e informed how s/he may withdraw the consent. Again, before doing so the company would carry out an impact assessment before proceeding to do so.

Information Technology

16. The company holds data electronically as identified in paragraph 12.

17. The company recognises that keeping accurate and up to date records is an integral part of all business activities. These records must be securely stored in the appropriate locations on the SAGE program and easily identifiable and accessible to those who need to see them. This means:
• Computer files must be maintained in a manner consistent with company protocols from time to time communicated and must be kept organised and up to date.
• Emails related to particular customers must be saved to the appropriate computer file and must not be stored solely in personal mail boxes.

18. All Data must not be retained or stored on a computer for longer than is necessary as set out in the policy.
In particular:
• Emails should only be retained for the period for which the retention is necessary for their use or information by the employee and deleted once that reason has expired.
• Documents may be saved in any network shared folders but only retained for the permitted purpose and for so long as the reason for obtaining/recording the information is necessary and should be deleted if either the permitted purpose has expired, and/or the information is no longer necessary. If the document relates to a customer, once the employee has finished working on the document this should be saved on the appropriate computer file and deleted from the network shared folder.
• Documents may be saved to desktop but only retained for the permitted purpose and for so long as the reason for obtaining/recording the information is necessary and should be deleted if either the permitted purpose has expired, and/or the information is no longer necessary. If the document relates to a customer, once the employee has finished working on the document this should be saved to the appropriate computer file and deleted from the desktop.

19. The use of memory sticks and other removable media is prohibited. Data must not be copied onto floppy disc, removable hard drive, CD or DVD or memory stick/thumb drive without the express permission of Phillip Mallinson and, should permission be given, it must be encrypted.

20. If permission should be granted, Data copied to any of these devices must be deleted as soon as possible and stored on the appropriate computer file in order for it to be backed up.

Retention of data

21. The company will only retain customer's data for a defined period of time before it is destroyed, namely:
(i) Payment / bank details will be destroyed as soon as possible after the data has been processed;
(ii) All other data relating to customers will be retained indefinitely although the company will regularly review this data and if it has not had any contact with any customer for three years will delete the data.
(iii) Data obtained by cookies on the company's website is retained for the periods set out in the company's cookie policy on its website.
(iv) For employee data please see the company's HR Policy.

22. The company will review the data it holds regularly and at least annually and destroy such data it no longer requires under paragraph 21. The person responsible for the review and destruction is Phillip Mallinson.

Right of information

23. The company's website contains a privacy notice which sets out information about the company which must be provided under the GDPR.

24. A copy of the privacy notice is given to every customer.

25. In addition, the privacy notice is exhibited on reception at the company's premises and copies are available on request.

26. The privacy notices set out in particular on what basis the company holds the data, what the company will do with the data obtained and how long the data will be retained for.

Right of access

27. Individuals have the right to obtain confirmation that their data is being processed and to request access to / copies of any data that the company holds in relation to them.

28. Phillip Mallinson is responsible for dealing with any access request. All employees must be alert to any access request and immediately notify Phillip Mallinson of any access request.

29. Phillip Mallinson will attend to any access request made as soon as possible and in any event within 28 days of the date or receipt of the same by the company.

30. Phillip Mallinson will record and keep an electronic record of all access requests received, including the date of receipt, the information / copies provided to the data subject, and the date of completion.

31. Phillip Mallinson will in conjunction with Linda Mallinson be responsible for determining;
(i) whether to respond to the access request by supplying the information or copies requested (as applicable);
(ii) if they determine to supply the information or copies requested, the extent of the same to be disclosed;
(iii) if they determine not to supply the information or copies requested, the reason why and will set the reasons out by way of written response to the data subject and explain that if the data subject does not agree that they have a right of recourse to the Information Commissioner and / or the courts;

(iv) if the request is manifestly unfounded or excessive and if so whether to charge an administration fee or to refuse the request;
(v) whether additional time over and above 28 days is required to deal with the request. If so determined, the data subject will be informed in writing and given an indication of when the request will be completed. In any event, the request will be attended to and completed within 84 days of the date of receipt;
(vi) whether evidence of the data subject's identity is required before disclosing the information or copies requested.

Right of rectification

32. The company acknowledges that it is obliged to ensure that all data is kept up to date and correct. The company will use its best endeavours to do so.
All employees are required to ensure that this is the case and if an employee becomes aware that any data is incorrect or out of date shall take immediate steps to ensure that the same is rectified and amended.

33. In the event of a request by a data subject to amend and / or rectify the data held, such request shall be referred by an employee immediately to Phillip Mallinson who shall take such reasonable steps to ensure that the rectification is justified and appropriate and shall then undertake the amendment as soon as possible (in relation to all data held relating to the said data subject) within 28 days. Phillip Mallinson shall then notify the data subject in writing of the rectification (or, if applicable, the reason why the data has not been rectified but in doing so shall explain that the data subject has a right of recourse to the Information Commissioner and / or the courts).

34. Phillip Mallinson will keep an electronic record of all requests for rectification made, including details of the request, the action taken and when.

Right of erasure

35. The company will only retain and process data relating to any individual for as long as is necessary and in line with the purpose for which the data was obtained and the provisions of this policy and the HR policy.

36. In the event that the company should receive any request for erasure by any individual Phillip Mallinson must be informed as soon as possible. Phillip Mallinson will decide whether the data of the individual in question can be erased. In doing so, he will take into account the purpose for which the data was obtained and the company's Policies relating to the retention of data. The individual will be notified in writing of the decision and the reason for the same. If the decision is that the data will not be erased, the individual will be informed of their right to complain to the Information Commissioner and / or the court.

If Phillip Mallinson decides that the data can be erased, he will arrange to do so within 28 days of determination. He will also notify any data processor who may hold or be processing the individual's data and seek confirmation from them also that the same has been deleted.

Employees' rights

37. Please refer to the HR Policy in relation to employees' data for access requests, rectification, erasure, restriction and portability.

Data Security

38. A breach of the GDPR occurs if there is a breach of security of data which leads to;
(i) accidental or unlawful destruction of;
(ii) loss of;
(iii) alteration of;
(iv) unauthorised disclosure or access to any data.

39. All employees have an ongoing obligation to comply with the GDPR. In the event that an employee should find that there has been a breach of the GDPR, or suspect that a breach of the GDPR may or is likely to have occurred, whether as a result of their own actions or the actions of someone else (including someone outside the company), a report must be made immediately (within 24 hours) to Philip Mallinson. All employees are obliged to make a report and to cooperate in providing any information that may be required by Philip Mallinson in order that they may deal with the breach / anticipated breach.

40. In addition, should a customer, employee or any third party allege or intimate that they are concerned that there is or may have been a breach of the GDPR, the employee must report immediately (within 24 hours) to Philip Mallinson.

41. If the breach is serious and relates to the security of the data of a customer, an employee, or any third party, which is also likely to result in a risk to the individual's rights and freedoms, Phillip Mallinson should be contacted by telephone in the first instance to advise that a breach has occurred.

42. Upon receipt of a report, Phillip Mallinson will give consideration to the matter raised, may request further information, and will decide whether the issue should be reported to the Information Commissioner's Office (ICO). In doing so, he will consider the likelihood and severity of the resulting risk to people's rights and freedoms. If that risk is identified, then he will notify the Information Commissioner within 72 hours.

43. Phillip Mallinson will also consider whether the individual/s affected should also be notified of the breach. He will consider whether the rights and freedoms of the individual/s have been affected, and the extent of the same, before deciding whether to inform them. If the decision is made to inform, then he will do so within 72 hours.

44. Phillip Mallinson will document the reason for the decision. Whether the breach is reported or not, the details will be retained and the report logged in the GDPR Register.

Data Protection by default

45. The company will ensure that compliance with the GDPR is inbuilt into its working systems and fabric of the businesses to ensure that data protection is considered and taken into account at all times.

46. The company will undertake a Data Protection Impact Assessment (DPIA) whenever the company should;
- elect or consider electing to use any new technology or technological process
- consider any extension to the retention periods for the storage of data
- consider any change to the type of data that it may hold
- elect or consider the use of cloud storage
  (over and above any existing cloud storage used)
- intend to use a new data processor
- consider a merger or acquisition

47. The extent of the DPIA will depend upon the change involved. A decision will be made by the company's managing director over who should be involved in the DPIA and who should be responsible for the same. The DPIA will be led by the individual responsible who shall determine the extent of the DPIA and what shall be required to be considered and documented.

48. Following the DPIA, the decision of the DPIA will be reviewed and approved by the company's Board before implementation.

Training

49. The company's managing director is responsible for training. The company intends to undertake and provide general training to all members of staff at least once every two years, although more frequent training will take place:
- If any breach of data protection is identified which requires to be reported
- A general failure of compliance with any aspect of the GDPR is identified
- If required by the Information Commissioner

- There is any material change to the GDPR and / or the company's Policies.

Data Processors

50. Where the company passes data to a third party for the purposes of processing the data upon its behalf, the company will ensure before doing so that it has entered into a written agreement with the Data Processor to regulate the use of the data. This shall include;
(i) specifically confirming the use of the data by the Data Processors;
(ii) how long the data may be retained for;
(iii) at the end of the period, whether the data should be destroyed or returned to the company;
(iv) the lawful basis upon which the company hold the data and that the data subject/s are aware that the data may be transferred to the data processor for processing;
(v) that the data may not be processed outside the EEA;
(vi) the appropriate security arrangements that the data processor must have in place and the obligation for the data processor to report any security breaches to the company immediately;
(vii) that the data processor will promptly assist the company in dealing with any data subject's rights;
(viii) recognition that the company is responsible for any actions of the data processor in relation to the use of the data and indemnity provisions.

51. The company maintains a central record of all Data Processors. The responsibility for and the upkeep of central record lies with the managing director.

52. In the event that any data should be transferred to a third party without a written agreement in place, the company will take all appropriate steps to obtain such written agreement and if the same should not be obtained within a reasonable period of time, but by at least 28 days, the company shall request the return of the data immediately and should the request not be complied with take appropriate action, whether by way of report to the Information Commissioner and / or application to the court for its return.

Employees duties in relation to confidentiality of data

53. Article 5 of the GDPR requires the company to have appropriate security to prevent data from being accidentally or deliberately compromised.

54. Computer Data in this policy means all data relating to the company or to its customers (whether held on paper or stored electronically on personal computers, mobile device or memory stick).

55. Computer Data remains at all times, the company's property.

56. At all times, the safeguarding of Computer Data is all employees' responsibility. Any loss of Computer Data or the dissemination of information within them is highly likely to amount to a breach of confidentiality and of the GDPR. If ever Computer Data should go missing, be destroyed or lost, this must be reported to the managing director as soon as possible. If stolen, or, being missing may have been stolen, employees must inform the Police immediately.

57. Employees must never leave any Computer Data unattended or in a vehicle. If the Computer Data is taken home or elsewhere for the purpose of work, it is the employee's responsibility to ensure that they are secure and that the contents or details are not released to any third party.

58. All and any Computer Data is strictly confidential. It is all employees' responsibility and duty to maintain confidentiality of this data at all times. This duty to maintain confidentiality continues after termination of employment.

Data Storage Facilities

59. The company will not store data outside the EEA.

Conclusion and Review

60. All employees and the company's obligations under the GDPR are extremely important. If Papers are destroyed, lost or stolen or data finds its way to any third party as a result of mishandling, negligence or neglect, this will lead to disciplinary proceedings and the company reserves the right to claim any losses incurred. Employees should note that in some circumstances it could amount to a criminal offence and / or a fine and / or sanction from the Information Commissioner's Office, and / or the court. If there is any breach of the Policies, then this may lead to disciplinary proceedings.

61. The Data Compliance Manager and Deputy Data Compliance Manager will review the Policies at least once every 12 months.