Privacy Policy
Employee and Job Applicant Data

1 About this Policy

1.1 Please read this policy because it gives important information about:

- the data protection principles with which Smeg UK must comply;
- what is meant by personal information (or data) and sensitive personal information (or data);
- how we gather, use and (ultimately) delete personal information and sensitive personal information in accordance with the data protection principles;
- where more detailed privacy information can be found, e.g. about the personal information we gather and use about you, how it is used, stored and transferred, for what purposes, the steps taken to keep that information secure and for how long it is kept;
- your rights and obligations in relation to data protection; and
- the consequences of failure to comply with this policy.

1.2 This policy does not form part of any employee's contract of employment and we may amend it at any time. We will circulate any new or modified policy to staff when it is adopted.

2 Who is Responsible for this Policy

2.1 The Human Resources Director is responsible for employee data protection compliance within Smeg UK. If you have any questions or comments about the content of this policy or if you need further information, you should contact the Human Resources Director at HR@smeguk.com.

3 Data Protection Introduction

3.1 We obtain, keep and use personal information (also referred to as data) about job applicants and about current and former employees, temporary and agency workers, contractors, interns, volunteers and apprentices for a number of specific lawful purposes, as set out in our data protection privacy notices (**Data Protection Privacy Notice - Employment**; **Data Protection Privacy Notice – Recruitment**) relating to recruitment and employment.

3.2 This policy sets out how we comply with our data protection obligations and seek to

protect personal information relating to our workforce. Its purpose is also to ensure that staff understand and comply with the rules governing the collection, use and deletion of personal information to which they may have access in the course of their work.

3.3 We are committed to complying with our data protection obligations, and to being concise, clear and transparent about how we obtain and use personal information relating to our workforce, and how (and when) we delete that information once it is no longer required.

4 Scope

4.1 This policy applies to the personal information of job applicants and current and former staff, including employees, temporary and agency workers, interns, volunteers and apprentices.

4.2 Staff should refer to the Data Protection Privacy Notices (**Data Protection Privacy Notice - Employment; Data Protection Privacy Notice – Recruitment**) and, where appropriate, to other relevant policies including in relation to information security, which contain further information regarding the protection of personal information in those contexts.

5 Definitions

5.1 **criminal records information** means personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures;

5.2 **data breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information;

5.3 **data subject** means the individual to whom the personal information relates;

5.4 **personal information** (sometimes known as personal data) means information relating to an individual who can be identified (directly or indirectly) from that information;

5.5 **processing information** means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with it;

5.6 **pseudonymised** means the process by which personal information is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that the personal information cannot be attributed to an identifiable individual;

5.7 **sensitive personal information** (sometimes known as 'special categories of personal data' or 'sensitive personal data') means personal information about an individual's

race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

6 Data protection principles

6.1 We will comply with the following data protection principles when processing personal information:

6.1.1 we will process personal information lawfully, fairly and in a transparent manner;

6.1.2 we will collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;

6.1.3 we will only process the personal information that is adequate, relevant and necessary for the relevant purposes;

6.1.4 we will keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal information are deleted or corrected without delay;

6.1.5 we will keep personal information for no longer than is necessary for the purposes for which the information is processed; and

6.1.6 we will take appropriate technical and organisational measures to ensure that personal information are kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

7 Basis for processing personal information

7.1 In relation to any processing activity we will, before the processing starts for the first time, and then regularly while it continues:

7.1.1 review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) for that processing, i.e.:

a) that the data subject has consented to the processing;

b) that the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

c) that the processing is necessary for compliance with a legal obligation to which Smeg UK is subject;

d) that the processing is necessary for the protection of the vital interests of the data subject or another natural person; or

e) that the processing is necessary for the purposes of legitimate interests of Smeg UK or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject.

7.1.2 except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose);

7.1.3 where sensitive personal information is processed, also identify a lawful special condition for processing that information (see paragraph 8.2.2 below), and document it; and

7.1.4 where criminal offence information is processed, also identify a lawful condition for processing that information, and document it.

8 Sensitive personal information

8.1 Sensitive personal information is sometimes referred to as ‘special categories of personal data’ or ‘sensitive personal data’.

8.2 We may from time to time need to process sensitive personal information. We will only process sensitive personal information if:

8.2.1 we have a lawful basis for doing so as set out in paragraph 7.1.1 above, e.g. it is necessary for the performance of the employment contract, to comply with our legal obligations or for the purposes of our legitimate interests; and

8.2.2 one of the special conditions for processing sensitive personal information applies, e.g:

a) the data subject has given has given explicit consent;

b) the processing is necessary for the purposes of exercising the employment law rights or obligations of Smeg UK or the data subject;

c) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;

d) processing relates to personal data which are manifestly made public by the data subject;

e) the processing is necessary for the establishment, exercise or defence of legal claims; or

f) the processing is necessary for reasons of substantial public interest.

8.3 Before processing any sensitive personal information, staff must notify the Human Resources Director of the proposed processing, in order that they may assess whether the processing complies with the criteria noted above.

9 Documentation and records

9.1 We will keep written records of processing activities which are high risk, i.e. which may result in a risk to individuals' rights and freedoms or involve sensitive personal information or criminal records information

9.2 We will conduct regular reviews of the personal information we process and update our documentation accordingly

10 Privacy notice

10.1 We will issue privacy notices from time to time, informing you about the personal information that we collect and hold relating to you, how you can expect your personal information to be used and for what purposes (HR.POL.Data Protection Privacy Notice - Employment; HR.POL.Data Protection Privacy Notice – Recruitment).

10.2 We will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

11 Individual rights

11.1 You have the following rights in relation to your personal information:

11.1.1 to be informed about how, why and on what basis that information is processed—see **Data Protection Privacy Notice - Employment; Data Protection Privacy Notice – Recruitment**.

11.1.2 to obtain confirmation that your information is being processed and to obtain

access to it and certain other information, by making a subject access request—see Subject Access Requests below;

11.1.3 to have data corrected if it is inaccurate or incomplete;

11.1.4 to have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as 'the right to be forgotten');

11.1.5 to restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased), or where the employer no longer needs the personal information but you require the data to establish, exercise or defend a legal claim; and

11.1.6 to restrict the processing of personal information temporarily where you do not think it is accurate (and the employer is verifying whether it is accurate), or where you have objected to the processing (and the employer is considering whether the organisation's legitimate grounds override your interests).

11.2 If you wish to exercise any of the rights in paragraphs 11.1.3 to 11.1.6, please contact the Human Resources Director.

12 Individual obligations

12.1 Individuals are responsible for helping Smeg UK keep their personal information up to date. You should the HR Self-Service System if the information you have provided to us changes, for example if you move house or change details of the bank or building society account to which you are paid.

12.2 You may have access to the personal information of other members of staff, and our suppliers and customers in the course of your employment or engagement. If so, we expect you to help meet its data protection obligations to those individuals. For example, you should be aware that they may also enjoy the rights set out in paragraph 11.1 above.

12.3 If you have access to personal information, you must:

12.3.1 only access the personal information that you have authority to access, and only for authorised purposes;

12.3.2 only allow other Smeg UK staff to access personal information if they have appropriate authorisation;

12.3.3 only allow individuals who are not Smeg UK staff to access personal information if you have specific authority to do so from the Human Resources Director;

12.3.4 keep personal information secure (e.g. by complying with rules on access to

premises, computer access, password protection and secure file storage and destruction and other precautions set out in the **IT & Communications Systems Policy**)

12.3.5 in accordance with the **IT & Communications Systems Policy** not remove personal information, or devices containing personal information (or which can be used to access it), from the premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device; and

12.3.6 not store personal information on local drives or on personal devices that are used for work purposes.

12.4 You should contact the Human Resources Director if you are concerned or suspect that one of the following has taken place (or is taking place or likely to take place):

12.4.1 processing of personal data without a lawful basis for its processing or, in the case of sensitive personal information, without one of the conditions in paragraph 8.2.2 being met;

12.4.2 any data breach as set out in paragraph 16.1 below;

12.4.3 access to personal information without the proper authorisation;

12.4.4 personal information not kept or deleted securely;

12.4.5 removal of personal information, or devices containing personal information (or which can be used to access it), from our premises without appropriate security measures being in place;

12.4.6 any other breach of this policy or of any of the data protection principles set out in paragraph 6.1 above.

12.5 From time to time Smeg may take promotional shots of employees for business marketing purposes. Smeg has a legitimate interest to take these photographs may use any such shots taken on the company premises or during demonstrations to customers etc. If an employee does not wish to have their photograph used for these purposes they must advise the HR Department (HR@smeguk.com).

13 Data Security

13.1 We will ensure that technical and organisational measures in accordance with the **IT and Communications Policy** to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

13.2 We have in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. We will only transfer personal data to third parties if they agree in writing to comply with those procedures and policies, or if they put in place adequate measures themselves.

13.3 Maintaining data security means guaranteeing the confidentiality, integrity and availability (for authorised purposes) of the personal data.

14 Providing Information to Third Parties

14.1 We will not disclose your personal data to a third party without your consent unless we are satisfied that they are legally entitled to do so in accordance with applicable laws. Where we do disclose your personal data to a third party, we will only do so in accordance with applicable data protection laws.

15 Storage and retention of personal information

15.1 Personal information (and sensitive personal information) will be kept securely in accordance with the Company's **IT & Communications Systems Policy**.

15.2 Personal information (and sensitive personal information) should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained.

15.3 Personal information (and sensitive personal information) that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

16 Data breaches

16.1 A data breach may take many different forms, for example:

- 16.1.1 loss or theft of data or equipment on which personal information is stored;
- 16.1.2 unauthorised access to or use of personal information either by a member of staff or third party;
- 16.1.3 loss of data resulting from an equipment or systems (including hardware and software) failure;
- 16.1.4 human error, such as accidental deletion or alteration of data;
- 16.1.5 unforeseen circumstances, such as a fire or flood;
- 16.1.6 deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and
- 16.1.7 'blagging' offences, where information is obtained by deceiving the organisation which holds it.

16.2 We will:

- 16.2.1 make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of

individuals; and

16.2.2 notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

17 International transfers

17.1 We will not transfer personal information outside the European Economic Area (EEA), which comprises the countries in the European Union and Iceland, Liechtenstein and Norway.

18 Training

18.1 We will ensure that staff are adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal information, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

19 Consequences of failing to comply

19.1 We take compliance with this policy very seriously. Failure to comply with the policy:

19.1.1 puts at risk the individuals whose personal information is being processed; and

19.1.2 carries the risk of significant civil and criminal sanctions for the individual and Smeg UK; and

19.1.3 may, in some circumstances, amount to a criminal offence by the individual.

19.2 Because of the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under our procedures, and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

20 Subject Access Requests

20.1 If you wish to know what personal data we hold about you, you must make the request in writing. All such written requests should be forwarded to the Human Resources Director.

21 Associated Documents

- QTY.PRO.Data Protection
- HR.PRO.Human Resources
- IT.POL.IT & Communications Systems Policy
- HR.POL.Data Protection Privacy Notice - Employment
- HR.POL.Data Protection Privacy Notice – Recruitment

Act	General Data Protection Regulation (GDPR) and The Data Protection Act 2018 (DPA)
Regulations	
Owner	Human Resources Director
Date Last Reviewed	19/04/2018