GRANTHAM CEILINGS & INTERIORS LTD

Data Protection Policy

Signed: ..... Ross Grant

Position: Managing Director

Date: 3 January 2019

Date for review: January 2020

Reference Points

- Data Protection Act 2018 and any subsequent legislation See https://www.gov.uk/data-protection/the-data-protection-act
- General Data Protection Regulations See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679
- Information Commissioners' Office
  See https://ico.org.uk/for-organisations/education/
- Subject Access Code of Practise
- The Use of Photographs and Electronic Images

The Data Protection Act (DPA) and the General Data Protection Regulations (GDPR) provide protection for individuals as to how their personal information is used by organisations, businesses or the government. Businesses are designated 'Data Controllers' and are required to keep records of processing activities, which must be made available to the Information Commissioner's Office upon request. Please see the links above for further information as to our responsibilities in relation to data protection.

Introduction

1.1. Grantham Ceilings and Interiors Ltd (GCI) collects and uses personal information about staff, sub-contractors and other individuals who come into contact with the business. This information is processed in order to enable GCI to provide interior construction, pay staff and sub-contractors plus other associated functions. In addition, there may be a legal requirement for GCI to process personal information to ensure that it complies with statutory obligations.

1.2. We have a duty, as a Data Controller, to keep detailed records of data processing activities and the records shall contain:-

- Name and details of the organisation (and where applicable, of other controllers, any representative and data protection officer)
- Purposes of the processing
- Description of the categories of individuals and categories of personal data.
- Categories of recipients of personal data
- Details of transfers to third countries including documentation of the transfer mechanism safeguards in place
- Retention schedules
- Description of technical and organisational security measures

These records must be made available to the Information Commissioner's Office (ICO) upon request. GCI will, on an annual basis, provide its registrable particulars and pay the data protection fee to the ICO.

2. Purpose

2.1. This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the GDPR and DPA and other related legislation. It will apply to personal information regardless of the way it is collected, used, recorded, stored and destroyed and irrespective of whether it is held in paper files or electronically.

2.2. All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines and shall undertake regular training to ensure compliance with their responsibilities.

3. Key principles

3.1 Personal information or data is defined as any information relating to an identifiable person who can be directly or indirectly identified by reference to an identifier held by the business.

3.1.1 Data Protection Principles – there are six enforceable principles contained in Article 5 of the General Data Protection Regulations. They are key to compliance and the business must endeavour to ensure that they are adhered to at all times. The responsibility for adherence to the principles is the responsibility+

3.1.2 of all staff of the business.

3.1.3 Principle 1 – Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.

3.1.4 Principle 2 – Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3.1.5 Principle 3 – Personal data shall be adequate, relevant and limited to what is necessary.

3.1.6 Principle 4 – Personal data shall be accurate and where necessary, kept up to date. Steps must be taken to ensure that personal data that is inaccurate is erased or rectified without delay.

3.1.7 Principle 5 - Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

3.1.8 Principle 6 - Personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage

3.2 To ensure compliance with the above principles the business will:

(a) Produce an information asset register that contains details of the records it holds.

(b) Inform individuals why the information is being collected at the point it is collected by way of privacy notices.

(c) Inform individuals when their information is shared, why and with whom it will be shared.

(d) Check the quality and the accuracy of the information it holds.

(e) Ensure that information is not retained for longer than is necessary.

(f) Ensure that when obsolete, information is destroyed and it is done so appropriately and securely.

(g) Create, maintain and publish a Disposal and Retention Schedule setting out retention and disposal dates for common data sets and other information.

(h) Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.

(i) Share information with others only when it is fair and lawful to do so and satisfies the lawful basis for processing that information.

(j) Share personal data with other organisations for the purpose of crime prevention and/or detection, or for the purpose of legal proceedings, provided that the disclosure falls within an exemption to the non-disclosure provisions contained within the Data Protection Act 2018 or any subsequent legislation.

(k) Disclose personal data where required to do so by law, for example, following receipt of a court order.

(l) Set out procedures to ensure compliance with the duty to respond to an individual's rights to:

- request access to personal information, known as Subject Access Requests.
- be informed about the way their data is used;
- have inaccurate personal data rectified;
- have their personal data erased;
- restrict the processing of their personal data; and
- object to the processing of their personal data.

(m) Ensure our staff are appropriately and regularly trained and aware of and understand our policies and procedures.

(n) Create and maintain a data breach notification spreadsheet to record data breaches and also circumstances where a breach was narrowly avoided.

4. Data Protection Officer (DPO)

4.1 Due to the size of the business, we are not required to have a DPO by law but any DP enquiries should be directed to Ross Grant, Managing Director, in the first instance.

5. Data Protection Impact Assessments (DPIA)

5.1 The business must carry out a DPIA when processing is likely to result in **high risk** to the rights and freedoms of individuals.

5.2 The GDPR does not define high risk but guidance highlights a number of factors that are likely to trigger the need for a DPIA, which include the use of new technologies, processing on a large scale, systematic monitoring, processing of special categories of personal data.

6. Privacy Notices

6.1 The business publishes a privacy notice on its website which provides information about how and why the business gathers and shares personal data.

6.2 The privacy notice under the GDPR should include:

- Who you are and how they can contact you;
- The personal data you are collecting & why you are collecting it;
- Where you get the personal data from & who you are sharing it with;
- How long the data will be held for;
- Transfers to third countries and safeguards;
- Description of the data subjects individual rights;
- The data subjects right to withdraw consent for the processing of their data; and
- How individuals can complain.

6.3 The privacy notice will be reviewed at regular intervals to ensure it reflects current processing.

6.4 The privacy notice will be amended to reflect any changes to the way the business processes personal data.

6.5 Whilst the business will publish an overarching privacy notice for sub-contractors, it will also issue a privacy notice to all staff members, before, or as soon as possible after, any personal data relating to them is obtained. This may simply be an explanation why the information is being requested and the purpose for which it will be used.

7 Photographs and Electronic Images

8.1 The business seeks consent to use images of sub-contractors in any business publicity material, its website, Facebook, Twitter, in published advertisements, brochures, articles and in training events.

9 Requests for Access to Personal Data

9.1 This section sets out the process that will be followed by the business when responding to requests for access to personal data made by a sub-contractor or member of staff.

9.2 Handling a subject access request for access to personal data:

9.2.1 Article 15 of the GDPR gives individuals the right to access personal data relating to them, processed by a data controller

9.2.2 Requests for information must be made in writing; which can include e-mail and be addressed to the Managing Director. If the original request does not clearly identify the information required, then the business will seek further enquiries to clarify what information is being requested.

9.2.3 The identity of the requestor must be established before the disclosure of any information is made. Below are some examples of documents which can be used to establish identity:

- Passport
- Driving licence
- Utility bill with current address
- Birth/marriage certificate
- P45/P60
- Credit card or mortgage statement.

9.2.4 The response time for a subject access request is one month from the date of the request (irrespective of business holiday periods). The one month period will not commence until any necessary clarification of information is sought. The time to respond can be extended to two months where the request is complex or numerous.

9.2.5 There are some exemptions available under the Data Protection Act which will mean that occasionally personal data will need to be redacted (information blacked out/removed) or withheld from the disclosure. All information will be reviewed prior to disclosure to ensure that the intended disclosure complies with the business's legal obligations.

9.2.6 Where the personal data also relates to another individual who can be identified from the information, the information will be redacted to remove the information that identifies the third party. If it is not possible to separate the information relating to the third party from the information relating to the subject of the request, consideration will be given to withholding the information from disclosure. These considerations can be complex and additional advice will be sought when necessary.

9.2.7 Where redaction has taken place then a full copy of the information provided will be retained in order to maintain a record of what was redacted and why and a clear explanation of any redactions will be provided in the business's response to the request.

9.2.8 If there are concerns about the disclosure of information additional advice will be sought.

11. Retention and Disposal of personal data

11.1 The business will ensure that it has an up to date and accurate retention and disposal schedule that is compliant with the GDPR. The business will ensure that personal data is stored, transferred and disposed of securely and in accordance with the retention and disposal schedule.

12. Security of personal data

12.1 The business will ensure that appropriate security measures are in place and enforced to keep paper and electronic personal data secure.

12.2 The business will regularly review the physical security of the business buildings and storage systems.

12.3 The business will ensure that only authorised individuals have access to personal data.

12.4 All portable electronic devices containing personal data will be encrypted.

12.5 No personal data will be left unattended in any vehicles and staff will ensure that if it is necessary to take personal data from business premises, for example to complete work from home, the data is suitably secured.

12.6 The business will refer to any relevant guidance and seek advice where necessary if processing personal data utilising a cloud based solution.

13. Complaints

13.1 Complaints relating to the business's compliance with the GDPR will be dealt with in accordance with the business's complaint policy.

13.2 Complaints relating to access to personal information should be made to Ross Grant, Managing Director, who will decide whether it is appropriate for the complaint to be dealt with through the business's complaints procedure. Complaints which are not appropriate to be dealt with through the business's complaints procedure can be referred to the Information Commissioner. Details of how to make a complaint to the ICO will be provided with the response letter. [Reference to the ICO should only usually be made where the business's internal complainants process has been exhausted]

13.3. Complaints relating to information handling may be referred to the Information Commissioner's Office (the statutory regulator). Contact details can be found on their website at www.ico.org.uk or telephone 01625 5457453

14. Review

14.1 This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months. The policy review will be undertaken by the Managing Director or nominated representative.

15. Contacts

15.1 If you have any enquiries in relation to this policy, please contact Ross Grant.

15.2 Further advice and information is available from the Information Commissioner's Office at www.ico.org.uk or telephone 01625 5457453