Roofglaze

Data Protection Policy

(GDPR) – Privacy Policy

The General Data Protection Regulations (GDPR) come into force on 25 May 2018 superseding the UK's Data Protection Act 1998 and it is a legal requirement for the Company to comply with the GDPR.

Therefore, it is the Company's policy to ensure any personal data held by us in whatever form be treated with sensitivity and privacy, as befits such information in respect of our employees, suppliers, customers and sub-contractors.

Roofglaze are registered with the Information Commissioners Office (ICO) to process information to enable the Company to provide manufacturing services, promote our goods and services, maintain our accounts and records and to support and manage our staff. We also process information using a CCTV system to maintain the security of the premises and for preventing and investigating crime.

The Company needs to keep certain information about its employees, suppliers, customers and sub-contractors for financial and commercial reasons to enable the monitoring of performance, to ensure legal compliance and for health and safety purposes.

In particular, this policy requires the Company's staff to consult the Data Protection Manager before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

Policy Scope
This policy applies to all subsidiaries of the Roofglaze Group of Companies all based at 11 Howard Road, Eaton Socon, St Neots, Cambridgeshire PE19 8ET, telephone number 01480 474797. You can find out more about us on our website www.roofglaze.co.uk.

The Board of Directors is ultimately responsible for ensuring that Roofglaze Group meets its legal obligations and seeks to protect personal data making sure that their staff understand the rules governing the use of personal data to which they may have access in the course of their work.

Data Protection Manager
To ensure the implementation of this policy the Company has designated Joan Watson as their Data Protection Manager. All enquiries relating to the holding of personal data should be referred to her in the first instance.

Version Number: 01
Issue Date: May 2018

General Staff Guidelines
Everyone who works for or with the Roofglaze Group of Companies has some responsibility for ensuring data is collected, stored and handled appropriately in accordance with the following working practices:

- personal data should not be disclosed to unauthorised people, either within the Company or externally;
- keep passwords secure, change them regularly and do not share your passwords with anyone in line with the Company's E-mail and Internet Policy;
- lock/log off computers when you are away from your desk;
- position computer screens away from windows to prevent accidental disclosures of personal information;
- ensure paper and printouts are not left where unauthorised people could see them, like on a printer;
- only authorised staff are permitted to take personal data offsite to perform their job function. In the case of personal data held on USB drives, laptops or personal computers staff should consult with our retained IT consultant to ensure that personal data is always encrypted;
- prevent virus attacks by taking care when you open emails and attachments or visit new websites;
- dispose of confidential paper waste securely by shredding or using the secure waste disposal bags available to be collected by the Company's approved waste disposal contractor;
- work on a "clear desk" basis by securely storing hard copy personal information when it is not being used;
- request help from your line manager or the data protection officer if you are unsure about any aspect of data protection;
- ensure visitors are signed in and out of the premises and accompanied where relevant in areas normally restricted to staff.

As an employee you are responsible for:

- checking that any information that you provide in connection with your employment is accurate and up-to-date;
- notifying the Company of any changes to information you have provided, for example changes of address;
- ensuring that you are familiar with and follow the Data Protection Policy.

You also need to know:

- that our ICT systems may be monitored including emails, website access and computer files on the server;
- to only collect the personal information you need for a particular business purpose;
- to update records promptly, for example changes of address, marketing preferences;
- to delete personal information the business no longer requires;
- that you can be prosecuted if you deliberately give out personal details without permission. Be wary of people who may try and trick you into giving out personal details. Identity checks should be carried out before disclosing personal information to either someone making an incoming call or when making outgoing calls. Also limited personal information must be given over the telephone and followed up with written confirmation if necessary;
- items which are marked "Personal" or "Private and Confidential", or which appear to be of a personal nature, are opened by the addressee only;
- if you use the Company's office address for matters that are not work-related, the Company cannot be responsible for the confidentiality of such items;
- any breach of the Data Protection Policy, either deliberate or through negligence, may lead to disciplinary action being taken and could in some cases result in a criminal prosecution.

Training
Managers must ensure staff are trained to comply with Data Protection and relevant legislation surrounding it, so they know what is expected of them. Training must be applicable to the roles and responsibilities the individual holds and training records must be kept.

Sensitive Personal Data
In most cases where the Company processes sensitive personal data they will require the data subject's explicit consent to do this unless exceptional circumstances apply, or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work).

Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

Accuracy and Relevance
The Company will ensure that any personal data they process is done lawfully, fairly and transparently.

The data collected on a subject should be adequate, relevant and limited to what is necessary in relation to the purposes for which it is being collected.

Personal data shall be accurate, where necessary kept up to date, and kept only for the period of time required to complete the processing task for which it is obtained.

Individuals may ask that the Company correct inaccurate personal data relating to them. If you believe that information held is inaccurate you should record the fact that the accuracy of the information is disputed and inform the Data Protection Manager in writing.

Access to Personal Data
Access to all personal data is restricted to limited staff.

Employment checks are carried out on personnel as applicable to their role and/or the service they are delivering. Employees will obtain Disclosure Barring Service checks and complete relevant security clearances as required.

Right to be Forgotten
A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

IT Security
Personal data stored electronically will be protected by the Company's security processes.

Access to all systems are restricted to limited employees as required for the application of their job role.

Only approved USB drives will be used by the Company's employees. All third-party USB drives must be checked by our retained IT consultant before they are used in our Company systems.

The Company operates an E-mail and Internet Policy, which defines appropriate and inappropriate use.

Roofglaze Group's Business Continuity arrangements identify how we will protect and recover the personal information we hold.

Transferring Data Internationally
There are restrictions on international transfers of personal data. You must not transfer personal data anywhere outside the EEA without first consulting the Data Protection Manager. Currently, the Roofglaze Group of Companies do not transfer any personal data outside the EEA.

Reporting Breaches
All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- investigate the failure and take remedial steps if necessary
- maintain a register of compliance failures
- notify the ICO of any compliance failures that are material either in their own right or as part of a pattern of failures

Any breach of the Data Protection Policy, either deliberate or through negligence, may lead to disciplinary action being taken and could in some cases result in a criminal prosecution.

Third Party Access to (Propeller Studios Limited) ICT Systems
With the exception of our primary IT support partner, access to the Company systems is restricted and can only be accessed as agreed with the System Administrator.

All other third-party providers are bound by confidentiality and security clauses within the service level agreements agreed.

Auto-enrolment Pension
Legal and General co-ordinate Roofglaze Group's auto-enrolment pension, but the personal information employees and the Company pass to them is restricted and bound by their confidentiality and security clauses.

Subject Access Requests
You are entitled to know what personal information the Company holds about you, why it is being held and who the Company discloses your information to.

All Subject Access Requests must be referred to the HR Manager in the first instance.

All Subject Access Requests will be dealt with in accordance with the current ICO Code of Practice on Subject Access.

Storage of Data
Hard copy personal data, whether related to our employees, suppliers, customers or sub-contractors is held in secure cabinets with access restricted to limited staff. This personal data is not routinely carried in transit however, where it is required to be transported, it will be held in secure containers.

Electronic personal information held locally will be held with restricted access to limited staff. Access will be controlled by means of user account control. This personal data is not routinely carried in transit however, where it is required to be transported, it will always be held on encrypted USB drives and not copied to an employee's personal computer.

Retention of Records and Data
For some records and data there are statutory retention periods with statutory authorities. For other records there are no statutory retention periods. However, there are either recommended retention periods or retention periods required by third party organisations.

The Company will retain records in accordance with the relevant authorities' recommendations and guidelines as per the addendum to our Data Protection Policy.

Disposal of Data
All hard copy personal data is securely shredded on-site by the Company's approved waste disposal contractor.

IT equipment including hard drives are disposed of in a secure manner by our IT consultant.

Obsolete and unused IT equipment is stored in the Company's secure server room with access restricted to limited personnel.

Electronic data is removed from our systems either through deletion or, if required, archiving. All archived records are securely stored with limited access.

Marketing
If we have received the appropriate consent from a customer, individual or company, then they may be contacted for marketing purposes and sent information and/or news that would be of interest to them. However, they will always have the option to unsubscribe from these communications at any time.

If, however, they have previously advised us that they do not want any information on our products and services sent to them, or to be included in any market research, then we will continue to respect their wishes.

Managers will always check our compliance with legal obligations such as copyright or licensing requirements when downloading or copying information, and when publishing documents.

Website
The Roofglaze Group's website is www.roofglaze.co.uk. We use Google Analytics on our website, which uses cookies to store visitor data and trends for its analytics services (which allows Roofglaze to view data about our website use and visitors). To see the data that Google Analytics use please refer to The Google Privacy Policy.

Overall, cookies help us to provide customers, individuals and companies with a better website and remember preferences. Individuals or companies can control and/or delete cookies as they wish – for details, see AboutCookies.org.

Cookies Policy
For details of the cookies that we use, please refer to the table contained within the Cookies Policy section on our website. Roofglaze is not responsible for the content or privacy policies of third parties or other websites.

Opting-out
Website visitors who do not want their data used by Google Analytics can install the Google Analytics opt-out browser add-on. To opt-out of Analytics for the web, visit the Google Analytics opt-out page and install the add-on for your browser.

Online Shop
We do not store entire credit/debit card numbers, nor do we keep a record of the security codes on customers' credit or debit cards. These details will only be requested during the processing of specific transactions.

Delivery Partners
In order for you to receive your goods, Roofglaze Group work with a number of delivery partners. Again, we only pass limited information to them in order to ensure delivery of your items.

Credit Reference Agencies
When you apply for credit with us we will make searches about you with credit reference agencies. We do this to make sure customers who apply for credit accounts are able to manage the level of credit offered and not committing fraud by providing false or inaccurate information.

In order to process your application we will supply your personal information to credit reference agencies and they will give us information about you, such as your financial history. We do this to assess your creditworthiness, check your identity, manage your account, trace and recover debts and prevent criminal activity.

The credit reference agencies that are currently used by the Roofglaze Group are:

- Experian.co.uk/
- Eulerhermes.co.uk/

Vehicle Tracking
It is essential to the business operation and to prevent fraudulent activities that all Company vehicles are installed with a tracking system. The Company has a legitimate interest in this to:

- prevent unauthorised fuel claims in relation to mileage travelled
- monitor vehicles to prevent theft for insurance purposes
- monitor unauthorised and unsafe out of hours use of vehicles
- protect staff, including a duty of care for driver safety and lone workers
- a need to track working hours against timesheets to ensure drivers comply with working time directives

The Right to Complain
If you wish to discuss your personal data or lodge a concern about the way in which it is handled, please contact our Data Protection Manager in the first instance.

The Right to Complain to the Supervisory Authority
If you are unhappy with any of the above detail, you have the right to complain to the Supervisory Authority, the details of which are below:

Supervisory Authority: Information Commissioner's Office (ICO)
Website: https://ico.org.uk/concerns/