GDPR POLICY

GENERAL DATA PROTECTION (GDPR) POLICY

We are transparent about how we collect and use the personal data of our colleagues, and to meeting our data protection obligations. This policy sets out our commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to the personal data of job applicants, employees, volunteers, apprentices and former employees, referred to as HR-related personal data.
This policy does not apply to the personal data of clients or other personal data processed for business purposes.

Gemma Bowers Chief People and Culture Officer is the person with responsibility for data protection compliance within the organisation. Questions about this policy, or requests for further information, should be directed to gemma.bowers@regularcleaning.com

DEFINITIONS

"Personal data" is any information that relates to a living individual who can be identified from that information.
"Processing" is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.
"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.
"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

DATA PROTECTION PRINCIPLES

We process HR-related personal data in accordance with the following data protection principles:

- We process personal data lawfully, fairly and in a transparent manner.
- We collect personal data only for specified, explicit and legitimate purposes.
- We process personal data only where it is adequate, relevant, and limited to what is necessary for the purposes of processing.
- We keep accurate personal data and take all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- We keep personal data only for the period necessary for processing.
- We take appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, accidental loss, destruction or damage.

We explain the reasons for processing personal data, how we use the data and the legal basis for processing in our privacy notices. We won't process your personal data for other reasons.

Where we rely on our legitimate interests as the basis for processing data, we carry out an assessment to ensure those interests are not overridden by your rights.

Where we process special categories of personal data or criminal records data to fulfil our own obligations or to exercise rights in employment law, this is done in accordance with a policy on special categories of data and criminal records data.

We update HR-related personal data promptly if an individual advises that their information has changed or is inaccurate.

Personal data gathered during employment, volunteering or apprenticeship is held in the individual's electronic personnel file. The length of time we hold HR-related personal data is detailed in our privacy notices. We keep a record of our processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

INDIVIDUAL RIGHTS

As a data subject, you have a number of rights in relation to your personal data.

SUBJECT ACCESS REQUESTS

You have the right to make a subject access request. If you make a subject access request, we will tell you:

- whether or not your data is processed and if so why, the categories of personal data we hold and the source of the data if it is not collected from you;
- who has access to your data and the safeguards in place when sharing the data;
- for how long your personal data is stored (or how that period is decided);
- your right to rectification or deletion of data, or to restrict or object to processing;
- your right to complain to the Information Commissioner if you think we have failed to comply with your data protection rights; and
- whether or not we carry out automated decision-making and the logic involved in any such decision-making.

We will also provide you with a copy of the personal data we process. This will normally be in electronic form if you make a request electronically, unless you agree otherwise.
If you want additional copies, we will charge a fee, which will be based on the administrative cost to us for providing additional copies.
To make a subject access request, you should send the request to people@regularcleaning.com or use our form to make a subject access request. In some cases, we may need to ask for proof of identification before the request can be processed. We will inform you if we need to confirm your identity and what documents we need.

We will normally respond to a request within a period of one month from the date it is received. In some cases, such as where we process large amounts of data, we may respond within three months of the date the request is received. We will write to you within one month of receiving the original request to tell you if this is the case.

If a subject access request is manifestly unfounded or excessive, we are not obliged to comply with it. Alternatively, we may agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which we have already responded. If you submit a request that is unfounded or excessive, we will notify you that this is the case and whether or not we will respond to it.

OTHER RIGHTS

You have a number of other rights in relation to your personal data. You can ask us to:

- correct inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if your interests override our legitimate grounds for processing data (where we rely on our legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not your interests override our legitimate grounds for processing data.

To ask us to take any of these steps, you should send your request to people@regularcleaning.com.

DATA SECURITY

We take the security of HR-related personal data seriously. We have internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

All existing and former employee data is held electronically on our CMS programme. Access to this data is only granted to the People and Culture team, Payroll and your line manager. Former employee electronic files are kept for 6 years with People and Culture and Payroll only having access. They are deleted after 6 years.

Where third parties process personal data on our behalf, they are required to demonstrate their confidentiality and must implement appropriate technical and organisational measures to ensure the security of data.

For further information please see our systems restrictions and data security policy.

IMPACT ASSESSMENTS

Some processing we carry out may result in risks to privacy. Where processing would result in a high risk to your rights and freedoms, we will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to lessen those risks.

DATA BREACHES

If we discover there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of individuals, we will report it to the Information Commissioner within 72 hours of discovery. We will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, we will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures we have taken.

INTERNATIONAL DATA TRANSFERS

We will not transfer HR-related personal data to countries outside the EEA.

INDIVIDUAL RESPONSIBILITIES

You are responsible for helping us keep your personal data up to date. You should let us know if data you have provided changes, for example if you move house or change bank details.
You may have access to the personal data of other individuals and of our clients in the course of your employment, volunteer period or apprenticeship. Where this is the case, we rely on you to help us meet our data protection obligations to staff and clients.

If you have access to personal data, you are required:

- to only access data that you have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);

- not to remove personal data, or devices that contain or can be used to access personal data, from the organisation's premises without following appropriate security measures (such as encryption or password protection) to secure the data and the device;
- not to store personal data on local drives or on personal devices that are used for work purposes; and
- to report data breaches, you are aware of to Gemma Bowers immediately.

Further details about the organisation's security procedures can be found in its data security policy.

Failing to observe these requirements may be treated as a disciplinary offence, which will be dealt with under our disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

TRAINING

As part of our commitment to our data protection responsibilities, Regular Cleaning will provide training to our colleagues to ensure we all comply to GDPR.

If your role requires regular access to personal data, you will receive additional training to help you understand your duties and how to comply with them.

Pauline Carrigan
Chair
2nd February 2023