



# JJ Cleaning Services

---

Part of JJ Group UK LTD

## Data Protection Policy

No part of this documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying or recording, for any purpose without express written permission of the CEO or head of operation of JJ Cleaning Services.

© 2025, JJ Cleaning Services a trading name of JJ Group UK LTD. All Rights Reserved

## Policy brief & purpose

Our **Company Data Protection Policy** refers to our commitment to treat information of employees, customers, stakeholders and other interested parties with the utmost care and confidentiality.

With this policy, we ensure that we gather, store and handle data fairly, transparently and with respect towards individual rights.

## Scope

This policy refers to all parties (employees, job candidates, customers, suppliers etc.) who provide any amount of information to us.

## Who is covered under the Data Protection Policy?

Employees of our company and its subsidiaries must follow this policy. Contractors, consultants, partners and any other external entity are also covered. Generally, our policy refers to anyone we collaborate with or acts on our behalf and may need occasional access to data.

## Policy elements

As part of our operations, we need to obtain and process information. This information includes any offline or online data that makes a person identifiable such as names, addresses, usernames and passwords, digital footprints, photographs, social security numbers, financial data etc.

Our company collects this information in a transparent way and only with the full cooperation and knowledge of interested parties. Once this information is available to us, the following rules apply.

Our data will be:

- Accurate and kept up-to-date
- Collected fairly and for lawful purposes only
- Processed by the company within its legal and moral boundaries
- Protected against any unauthorized or illegal access by internal or external parties

Our data will not be:

- Communicated informally
- Stored for more than a specified amount of time
- Transferred to organizations, states or countries that do not have adequate data protection policies
- Distributed to any party other than the ones agreed upon by the data's owner (exempting legitimate requests from law enforcement authorities)

In addition to ways of handling the data the company has direct obligations towards people to whom the data belongs. Specifically we must:

- Let people know which of their data is collected
- Inform people about how we'll process their data
- Inform people about who has access to their information
- Have provisions in cases of lost, corrupted or compromised data
- Allow people to request that we modify, erase, reduce or correct data contained in our databases

## **Actions**

To exercise data protection we're committed to:

- Restrict and monitor access to sensitive data
- Develop transparent data collection procedures
- Train employees in online privacy and security measures
- Build secure networks to protect online data from cyberattacks
- Establish clear procedures for reporting privacy breaches or data misuse
- Include contract clauses or communicate statements on how we handle data
- Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorization etc.)

Our data protection provisions will appear on our website.

## **Disciplinary Consequences**

All principles described in this policy must be strictly followed. A breach of data protection guidelines will invoke disciplinary and possibly legal action.

## **Roles and Responsibilities**

### **Data Protection Officer**

The Data Protection Officer (DPO) is responsible for:

- overseeing the implementation of this policy;
- monitoring the group's overall compliance with this policy and data protection law;
- advising on the development of related policies, procedures and guidelines;
- supporting with:
  - Data Protection Impact Assessments;
  - The investigation of reported data breaches;
  - The management of data subject requests;
  - The management of information requests;

- Data processor compliance checks; and
  - The completion of data protection impact assessments.
- acting as a contact point for data subjects and the supervisory authority; and
- reporting on their activities, including any advice and recommendations about any data protection issues, directly to the CEO.

The DPO role is currently held by Jake Ali, who can be contacted by email at [Jake.Ali@JJCleaningServices.uk](mailto:Jake.Ali@JJCleaningServices.uk).

## All colleagues

All colleagues are responsible for:

- Processing personal data in line with this policy, any associated guidance and any supplementary procedures that may be issued, including:
  - Locking computers when they are not in use.
- Maintaining personal data held in our centrally approved systems to ensure they are kept accurate and up to date
- Informing their Line Manager, or updating the Employee Self-Service system, about any relevant changes to their own personal data, such as a change of address (for example);
- Fully participating in all data protection training arranged for them, including any updated guidance that is issued by JJ Cleaning Services part of JJ Group UK LTD
- Cooperating with any reasonable request for involvement in compliance monitoring;
- Reporting any personal data breach as soon as they become aware of it, in line with the reporting data breaches section of this policy;
- Ensuring data protection issues are considered before they procure any new service.
- Notifying the DPO if they:
  - Have any questions about the operation of this policy or data protection law;
  - Have any concerns that this policy is not being followed;
  - Are unsure whether they can use personal data in a particular way; or
  - Receive a request from an individual to exercise their rights.

## Disposing of personal data

We will only retain personal data for as long as we need it in order to fulfil the purposes for which it was processed. We will maintain a retention schedule to outline how long we will keep different types of personal data. Our retention schedule will be reviewed at least once every two years.

Once personal data is no longer needed, we will dispose of it securely. Disposal methods include:

- shredding or incineration for paper records;
- deleting or overwriting electronic records; and
- physical destruction of old devices, drives, disks and other media.