TOTAL CARE CLEANING LTD

CONFIDENTIALITY & DATA PROTECTION POLICY

Document Ref: TCC-IMS-POL-DP-001
Version: 1.0

Date 03/06/2025
Approved By: Director
Applies To: All employees, subcontractors, agency staff, and temporary workers
Review Frequency: 12 months

---

1. Purpose

Total Care Cleaning Ltd is committed to protecting confidentiality and ensuring that all personal data and client information is handled lawfully, securely, and responsibly. This policy sets out how the Organisation manages confidential information and complies with UK data protection requirements while delivering cleaning services.

---

2. Scope

This policy applies to:

- All staff working for or representing Total Care Cleaning Ltd
- All client sites and locations where services are delivered
- All personal data processed in relation to employees, clients, and members of the public
- All formats of information including paper, digital systems, emails, photos, CCTV-related observations, and verbal information

---

3. Policy Statement

Total Care Cleaning Ltd will:

- Protect confidential information belonging to clients, service users, and employees
- Only collect and use personal data for legitimate business reasons
- Maintain appropriate security and access controls
- Prevent unauthorised disclosure or misuse of data

- Report and manage suspected data breaches promptly
- Provide staff training and enforce compliance through supervision and disciplinary controls

---

4. Definitions

Confidential Information

Any information that is not publicly available and relates to:

- Clients, their staff, service users, or buildings
- School pupils, vulnerable persons or medical/service user information
- Business operations, pricing, contracts, passwords, or access procedures
- Cleaning schedules, security arrangements, alarm codes, or keys

Personal Data

Any information relating to an identifiable person (e.g., name, address, phone number, email).

Special Category Data

Sensitive personal data such as health details, ethnicity, or safeguarding-related information (high protection required).

Data Breach

A security incident resulting in accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access to personal data.

---

5. Responsibilities

5.1 Director / Senior Management

Responsible for:

- Ensuring adequate resources for data protection compliance
- Approving and reviewing this policy
- Ensuring breaches and incidents are investigated and resolved

5.2 Supervisors / Managers

Responsible for:

- Ensuring staff follow confidentiality rules on client sites
- Reporting and escalating suspected breaches immediately
- Controlling access to keys, fobs, codes, and client documents

5.3 Employees / Workers

Responsible for:

- Maintaining confidentiality at all times
- Only accessing information necessary for their role
- Reporting concerns, loss, theft, or breaches immediately
- Following client site rules and Total Care Cleaning Ltd procedures

---

6. Confidentiality Rules (Cleaning Staff and Site Conduct)

All employees must:

✅ Keep all client and site information private
✅ Only discuss work information with authorised individuals
✅ Follow site security rules, sign-in procedures, and restricted areas
✅ Keep keys, codes, and access devices secure at all times
✅ Report suspicious behaviour or information exposure immediately

Employees must NOT:

❌ Read client paperwork, student files, HR documents, or medical information
❌ Open drawers, cupboards, files, or IT systems unless instructed and authorised
❌ Take photos or videos on site without written permission
❌ Share staff names, rotas, or security arrangements with anyone not authorised
❌ Post photos or information about client sites on social media
❌ Use client devices (computers/printers) without explicit approval
❌ Remove any client documents from site

---

7. Data Protection Principles (UK GDPR Aligned)

Total Care Cleaning Ltd will ensure personal data is handled in accordance with key data protection principles:

- **Lawfulness, fairness and transparency**

- **Purpose limitation** (only use data for the reason collected)
- **Data minimisation** (only collect what is needed)
- **Accuracy** (keep information correct and updated)
- **Storage limitation** (retain only as long as required)
- **Integrity and confidentiality** (secure handling)
- **Accountability** (able to demonstrate compliance)

---

8. Handling Personal Data in Practice

8.1 What personal data we may process

Examples include:

- Employee records (name, address, emergency contacts, training records)
- DBS status and safeguarding suitability (where applicable)
- Client contacts and site instructions
- Incident and accident reports
- Complaints and investigation records

8.2 Access controls

Personal data will only be accessed by:

- authorised managers
- HR/admin personnel
- supervisors where required for operations
- the client where contractually required

---

9. Secure Storage and Information Control

Total Care Cleaning Ltd will maintain security controls including:

Paper Records

- Stored in locked cabinets or secure offices
- Not left unattended on desks or vehicles
- Transported only when necessary

Digital Records

- Stored on secure systems and/or password protected devices
- Limited access permissions
- Regular backups where appropriate
- No saving sensitive information onto personal devices

Vehicles (Important for cleaning operations)

- Site keys, documents, and chemicals must not be left visible or unsecured
- Any site documentation must be kept locked away when not in use

---

10. Email, Messaging and Mobile Phone Use

Staff must ensure:

✅ Work information is shared only via authorised channels
✅ Emails include only necessary information
✅ Personal data is not shared by WhatsApp/text unless authorised and necessary
✅ Devices are protected with passcodes / lock screens
✅ Lost/stolen devices are reported immediately

---

11. Photographs, CCTV, and Recording

No employee may take photographs or videos on client sites unless:

- The client has given written approval
- It is required for reporting a defect/damage/incident
- It is stored securely and shared only with authorised persons

Photographs must never include:

- children or vulnerable adults
- personal information visible on screens/documents
- safeguarding-sensitive environments

---

12. Data Breach and Incident Reporting

Any suspected data breach must be reported immediately to management.

Examples include:

- Lost keys/fobs with identifiable site details
- Sending an email to the wrong recipient
- Leaving client paperwork unsecured
- A stolen phone containing client information
- Discussing confidential information publicly
- Unauthorised access to personal data

Immediate actions:

1. Report to Supervisor/Manager immediately
2. Contain the breach (recover items, secure access, change codes if required)
3. Record incident details
4. Management investigates and decides escalation actions

---

13. Disciplinary Action

Breaches of confidentiality and data protection may result in:

- removal from site
- investigation
- disciplinary action up to dismissal
- potential legal consequences depending on severity

---

14. Training and Awareness

All staff will receive confidentiality and data protection training through:

- induction
- toolbox talks
- refresher training when required
- client site-specific rules (e.g., schools)

Evidence will be retained in the Training Matrix and induction sign-off.

---

15. Monitoring and Review

Compliance will be monitored by:

- site supervision and audits
- incident trend monitoring
- internal audits
- management review

This policy is reviewed annually or following:

- significant breaches
- client complaints
- legal/regulatory changes

Signed,

Byron Phillips-Noble
Director
Total Care Cleaning Ltd