



PriorityWaste[®]

Your waste is our priority

PRIORITY WASTE – CONFIDENTIALITY POLICY

Version: 2.0

Issued: 23/09/25

Approved By: Gary Cronnolley – Compliance & Sales Director

Next Review: 23/09/26

1. Purpose

1.1 This Confidentiality Policy sets out how Priority Waste Limited protects confidential information belonging to the business, its customers, suppliers and employees.

1.2 The purpose of this policy is to:

- Ensure all confidential information is handled securely and responsibly.
- Protect commercial interests and customer trust.
- Support compliance with UK data protection law and contractual obligations.
- Make clear the responsibilities of all staff and contractors.

2. Scope

2.1 This policy applies to:

- All employees, temporary staff, agency workers and contractors.
- All locations (office, warehouse, homeworking, vehicles, customer sites).
- All forms of information (written, digital, verbal, audio, visual).

2.2 This policy should be read alongside the following:

- Data Protection Policy.
- Monitoring & Surveillance Policy.
- Remote Working & Homeworking Policy.
- IT and Communications / Email / Internet / Social Media Policy.

3. Definitions

3.1 “Confidential Information” includes (but is not limited to):

- Customer details and contact information.
- Customer pricing, margins, quotes and contracts.
- Supplier terms, pricing and rebates.

- Hazardous waste information (including types, quantities, site details).
- Financial information, invoices, credit terms, banking details.
- Internal procedures, SOPs, policies, training materials.
- Staff information (HR records, performance, payroll).
- System logins, passwords and internal portal data.

3.2 “Personal Data” means any information relating to an identifiable individual, as defined by UK data protection law. Personal data may also be confidential.

4. Responsibilities

4.1 Company (Priority Waste):

- Provide clear guidance and training on confidentiality.
- Put in place controls to protect confidential information.
- Investigate suspected or actual breaches.

4.2 Managers and Supervisors:

- Lead by example in protecting confidential information.
- Ensure staff in their team understand and follow this policy.
- Escalate any suspected confidentiality issues immediately.

4.3 All Employees and Contractors:

- Treat all confidential information with care and discretion.
- Only access information they genuinely need for their role.
- Never disclose confidential information without proper authority.
- Report any suspected breach or loss of information immediately.

5. Use and Disclosure of Confidential Information

5.1 Confidential information may only be used for legitimate business purposes and only where necessary for the person’s role.

5.2 Employees must not:

- Share confidential information with unauthorised colleagues.
- Discuss confidential matters in public places (reception, corridors, vehicles, cafés, public transport).
- Disclose confidential information to friends, family or other third parties.
- Post confidential information on social media, messaging apps or personal email.

5.3 Confidential information may only be shared with:

- Authorised staff within Priority Waste on a “need to know” basis.

- Approved third parties (suppliers, contractors, regulators) where:
 - It is necessary for the service, and
 - There is a contract or NDA in place where appropriate.

5.4 If in doubt whether information can be shared, staff must check with their manager or the Compliance & Sales Director before disclosing anything.

6. Storage and Handling of Confidential Information

6.1 Paper records:

- Must be kept in secure filing cabinets or offices when not in use.
- Must not be left unattended on desks, in reception, in vehicles or in public areas.
- Must be transported in a way that prevents loss or unauthorised viewing.

6.2 Electronic records:

- Must be stored only on authorised systems (e.g. company server, portals, approved cloud systems).
- Must not be stored on personal USB sticks or personal cloud accounts.
- Devices (laptops, tablets, phones) must be password protected and locked when unattended.

6.3 On vehicles and customer sites:

- Consignment notes, WTNs and other documentation must be kept secure in the vehicle and out of public view.
- Documents must not be left in customer areas where they can be accessed or photographed.

6.4 Remote working / homeworking:

- Screens must not be visible to others who do not work for Priority Waste.
- Any printed documents must be stored safely at home and not mixed with personal paperwork.

7. Verbal Communication

7.1 Employees must:

- Take care when speaking about customers, suppliers or internal issues in open offices, reception areas or on the phone.
- Confirm the identity of the person they are speaking to if confidential information is discussed.
- Avoid reading out full account numbers, payment details or sensitive information where it could be overheard.

8. Confidentiality and Personal Data

8.1 Where confidential information includes personal data, the Data Protection Policy also applies.

8.2 Staff must:

- Only access personal data where needed for their role.
- Not export or copy personal data to personal devices or apps.
- Follow all security procedures for storing and transmitting personal data.

9. Third Parties, Suppliers and Visitors

9.1 Confidential information must not be shared with third parties unless:

- It is necessary for the service they provide.
- They are approved by management.
- Where appropriate, a confidentiality clause or NDA is in place.

9.2 Visitors must not have unsupervised access to documents, screens or systems showing confidential information.

10. Leaving Priority Waste / Change of Role

10.1 When an employee leaves the company or changes role:

- Access to systems will be removed or amended.
- Any company devices, documents, notebooks, USB sticks or records must be returned.

10.2 Employees remain bound by confidentiality obligations after leaving the company. They must not:

- Use confidential information for their own benefit or for another business.
- Share confidential information with new employers or any other party.

11. Breaches of Confidentiality

11.1 Examples of confidentiality breaches include (but are not limited to):

- Sending information to the wrong recipient.
- Discussing a customer's account with an unauthorised person.
- Losing paperwork containing confidential information.
- Storing or sending confidential information using unauthorised apps or devices.

11.2 Any suspected or actual breach must be reported immediately to:

- The relevant line manager, and
- Gary Cronnolley (Compliance & Sales Director).

11.3 Breaches will be investigated and may result in:

- Corrective action (e.g. process changes, training).

- Disciplinary action, up to and including dismissal in serious cases.
- Notification to affected customers, suppliers or regulators where required.

12. Training and Awareness

12.1 All new starters will receive training on confidentiality during induction.

12.2 Refresher training will be provided where:

- There are changes to law or practice.
- A breach or near-miss highlights a training need.

12.3 Staff are expected to ask for guidance if they are unsure how to handle specific information.

13. Policy Review

13.1 This policy will be reviewed annually or sooner if:

- There are changes in legislation or regulation.
- There are significant changes to systems or working practices.
- An incident highlights the need for an update.

14 Acknowledgement

All employees must read and understand this policy and follow the PPE requirements at all times.

Signed:



Gary Cronnolley
Compliance & Sales Director
Priority Waste Limited

Date: 23rd September 2025