HIGHLANDER
INTERNATIONAL RECYCLING
Your Gateway to World Recycling Markets

DATA PROTECTION POLICY STATEMENT

Highlander are fully committed to compliance with the requirements of Data Protection Laws, and GDPR.

Protection of Personal Data

Care must be taken to ensure all staff comply with Data Protection regulations. All staff must ensure personal data is controlled and secure and details are not disclosed to any other person (whether inside or outside the company) unless authorised to do so. To ensure staff are aware of data protection obligations and information security we have a training programme in place and all staff are made aware of this policy, our Privacy policy and other relevant company policies

Compliance with Data Protection Regulations

To ensure we are compliant with data protection regulations including General Data Protection Regulation (GDPR) the company has taken various measures to ensure we are meeting all requirements;

- **Data Protection Officer** – Our management system details key responsibilities including details of our Data Protection Officer.
- **Personal Data Collected** – We do not actively collect or process any personal information other than the details of our employees, which is held securely, with prior consent, and only authorised staff members have access to this information. We may also hold some personal data from interactions with prospective and existing customers and systems are in place to manage this data, however most of this is business data.
- **Data Review** - we regularly review and check Personal data by completing a data audit to identify *"any information relating to an identified or identifiable natural person (data subject)",* to ensure the personal data we hold is required, lawfully managed and processed, as well as being accurate.
- **Data Retention** - Data retention is managed and retention period is documented in our management system manual.
- **Consent** - If any data is to be collected for any purpose other than normal employment purposes we will obtain your explicit consent and you have the right to withdraw this consent at any time.

- **Sensitive Personal Data** – This type of data is only held if there is a valid, legal reason to do so, and this information is treated with upmost security, and in line with data protection laws & regulations.
- **Privacy by Design** - Any new developments, projects or technologies that involve personal data will be reviewed to ensure privacy by design and privacy impact assessment completed.
- **Data Processing -** Personal data is processed and handled in a lawful and transparent manner with clear communication of what data we hold, why we hold it and how long we retain it. In terms of personal data collected on behalf of our shredding clients, this is all handled in line with our shredding procedures, EN15713 accreditation, as well as UKSSA Code of Practice.
- **Data Transfer** - We will not transfer personal data to any third parties except to those approved for the purposes of taxation, pension, employee checks, payroll administration and IT support.
- **International Transfer of Data** – we will not transfer your data internationally and will inform data subjects in any event of international transfer.
- **Data Security** - we have measures in place to protect confidentiality, integrity and accessibility of all company data and complete regular audits and reviews of the security of personal data & information security systems. All employees sign a Deed of Confidentiality on commencement of employment, and suppliers/contractors sign a non-disclosure agreement.
- **Company devices** – Any company devices issued to staff are purely for business purposes and acceptable use of these devices is stipulated within the staff handbook.
- **Data Subject Access** – Data subjects have the right to access, correct, transfer or request deletion of the personal data we hold about them. We will respond to all data requests within 1 month. We will not charge for responding to such requests.
- **Data Breaches** – All data breaches will be reported internally, and logged under non-conformance for investigation. Significant breaches will be reported to the ICO and affected data subjects notified within 72 hours of discovery.

Much of the arrangements for management of data, documented information, and ongoing checks including internal audits are all covered by our ISO 9001 compliant integrated

management system which is available to all staff. Our management system documentation includes the following;

- Summary of all company procedures and policies relating to Data management / Security
- Organisation details including details of the each person's responsibilities
- Document register detailing what records we hold, how they are managed and retention period
- Personal Data Audit & Internal audit of Data / Data Protection & Information Security
- Training arrangements including details of planned training and staff training / competency matrix

Highlander regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between the company and those with whom it carries out business. The company will ensure that it treats personal information lawfully and correctly.

To this end the company fully endorses and adheres to the Principles of Data Protection as set out in GDPR.

Signed May 2019
Joint Managing Directors

Brian Bingham

Stephen Duffy