Data Protection Policy

Definitions

Business	Dauson Environmental Group
DPA	Means Data Protection Act 2018, UK implementation of the EU GDPR.
GDPR	means the General Data Protection Regulation.
Responsible Person	means 'Head - HR, Health & Safety & Quality'
Register of Systems	means a register of all systems or contexts in which personal data is processed by the Business.

Data protection principles

The Business is committed to processing personal data in accordance with its responsibilities under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Article 5 of the UK GDPR requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;

b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d. accurate and, where necessary, kept up to date;

e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; and

f. processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

General provisions

a. This policy applies to all personal data processed by the Business.

b. The Responsible Person shall be responsible for monitoring compliance with this policy and applicable data protection legislation.

c. This policy shall be reviewed at least annually and whenever there are significant changes to legislation, guidance, business operations or processing activities.

Lawful, fair and transparent processing

a. The Business shall maintain a Record of Processing Activities (ROPA) detailing all personal data processing activities undertaken by the organisation.

b. The ROPA shall be reviewed and updated whenever processing activities change and, as a minimum, annually.

c. Privacy notices shall be provided where personal data is collected, explaining how personal data will be used, the lawful basis for processing, retention periods and individual rights.

d. The Business shall process personal data only where a lawful basis exists under UK GDPR.

Lawful purposes

a. All personal data processed by the Business shall be processed under one or more of the following lawful bases:

   • Consent
   • Contract
   • Legal obligation
   • Vital interests
   • Public task
   • Legitimate interests

b. The lawful basis for each processing activity shall be recorded within the ROPA.

c. Where consent is relied upon, records of consent shall be maintained.

d. Individuals shall be able to withdraw consent easily, and systems shall ensure that such withdrawals are actioned promptly.

Data minimisation

a. The Business shall ensure that personal data collected is adequate, relevant and limited to what is necessary for the purposes for which it is processed.

b. Personal data shall not be collected merely because it may be useful in the future.

c. Periodic reviews shall be undertaken to identify and remove unnecessary personal data.

Accuracy

a. The Business shall take reasonable steps to ensure personal data remains accurate and up to date.

b. Individuals shall be provided with mechanisms to update or correct their personal information.

c. Inaccurate personal data shall be corrected or deleted without undue delay.

Data Subject Rights and Access to Information

The Business recognises the rights of individuals under UK GDPR and shall implement procedures to facilitate the exercise of those rights.

Individuals have the right to:

• Be informed about the collection and use of their personal data.

• Access their personal data.

• Request rectification of inaccurate personal data.

• Request erasure of personal data where appropriate.

• Restrict processing in certain circumstances.

• Object to processing where applicable.

• Request data portability where applicable.

• Not be subject to solely automated decision-making where prohibited by law.

Subject Access Requests (SARs)

a. Requests may be submitted verbally or in writing.

b. Requests may be submitted verbally or in writing.

c. All requests shall be forwarded immediately to the Responsible Person.

d. The identity of the requester shall be verified before information is disclosed.

e. Responses shall be provided without undue delay and within one month of receipt unless an extension is permitted by law.

f. Records of requests, decisions and responses shall be retained to demonstrate compliance.

Data Retention and Secure Deletion

a. The Business shall maintain a Data Retention Schedule identifying categories of personal data, retention periods and disposal requirements.

b. Personal data shall be retained only for as long as necessary to fulfil the purpose for which it was collected or to meet legal, regulatory or contractual obligations.

c. Retention periods shall be reviewed annually.

d. Once retention periods expire, personal data shall be securely deleted, destroyed or anonymised.

e. Electronic records shall be permanently deleted using appropriate methods designed to prevent recovery.

f. Paper records containing personal data shall be disposed of through secure shredding or approved confidential waste services.

g. Personal data retained within system backups shall be managed in accordance with backup retention schedules and shall not be restored except where necessary for disaster recovery purposes.

Record of Processing Activities (ROPA)

a. The Business shall maintain a Record of Processing Activities (ROPA) as required by UK GDPR.

b. The ROPA shall include:

- The purposes of processing.
- Categories of data subjects.
- Categories of personal data processed.
- Lawful bases for processing.
- Categories of recipients.
- Details of international data transfers.
- Retention periods.
- Technical and organisational security measures.

c. The Responsible Person shall ensure the ROPA remains accurate and up to date.

Security

a. The Business shall implement appropriate technical and organisational measures to safeguard personal data.

b. Access to personal data shall be restricted to authorised personnel with a legitimate business need.

c. Systems containing personal data shall be protected through appropriate access controls, passwords, encryption and security updates where applicable.

d. When personal data is deleted, appropriate measures shall be taken to ensure the information cannot be recovered.

e. Appropriate backup, disaster recovery and business continuity arrangements shall be maintained.

f. Employees and contractors with access to personal data shall receive appropriate training and awareness on data protection responsibilities

Data Breach

In the event of a personal data breach, the Business shall:

a. Investigate the breach promptly and assess the potential impact on individuals' rights and freedoms.

b. Maintain a record of all personal data breaches, regardless of whether they are reportable.

c. Notify the ICO without undue delay and, where feasible, within 72 hours where the breach is likely to result in a risk to the rights and freedoms of individuals.

d. Notify affected individuals without undue delay where the breach is likely to result in a high risk to their rights and freedoms.

e. Implement corrective actions to prevent recurrence.

Name: David Neal

Date: May 2026

Position: Director

Signature:

Next review: May 2027

