Data Protection Policy

Policy

Back-To-Your-Roots.co.uk will at all times respect the confidentiality of any personal data and is committed to processing data in accordance with its responsibilities under the GDPR.

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

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes, or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

General Provisions

1. This policy applies to all personal data processed by BackToYourRoots.co.uk.
2. The Responsible Person shall take responsibility for the Organisation's ongoing compliance with this policy
3. The Responsible Person shall be the Organisation's designated person.
4. If required, the Organisation shall register with the Information Commissioner's Office and/or the GDPR as an organisation that processes personal data.

We manage our records by:

- Keeping records secure - e.g. by locking paper records in a filing cabinet and using passwords to protect data held on computers.
- Ensuring only appropriate, authorised staff with the necessary training have access to employment records.
- Not giving a reference about a current or ex staff member without gaining their consent.
- Ensuring records are disposed of securely - e.g. by shredding manually or electronically.

Lawful, Fair and Transparent Processing

Individuals have the right to access their personal data and any such requests made to the Organisation shall be dealt with in a timely manner (requests about the data stored about individuals should be made in writing to the Responsible Person by the individual).

Data Minimisation

The Organisation shall ensure that personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Accuracy

The Organisation shall take reasonable steps to ensure personal data is accurate.

Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

Archiving, Removal and Anonymisation

To ensure that personal data is kept for no longer than necessary, the Organisation shall put in place archiving/removal/anonymisation processes for each area in which personal data is processed and review these process annually.

The archiving/removal/anonymisation processes shall consider what data should/must be retained, for how long, and why.

Data Security

The Organisation shall ensure that personal data is stored securely and all computers are using anti-virus software that is up-to-date.

Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.

When personal data is deleted this should be done safely so that the data is irrecoverable.

Appropriate backup and disaster recovery solutions shall be in place.

Data Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Organisation shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO.

Any member of staff who inappropriately passes on confidential information will be subject to disciplinary action.