DATA SECURITY AND RETENTION POLICY

1. Introduction

1.1. This Data Security and Retention Policy should be read in conjunction with our other data protection documents including our, Privacy Notice and Cookies Policy, Data Protection Policy – Staff and Data Protection Policy – Volunteers and Trustees.

1.2. We are committed to complying with our obligations under the Data Protection Act 2018 (DPA) and the UK General Data Protection Regulation (GDPR).

1.3. It is a tool used to assist us in making decisions on whether a particular document should be retained or disposed of. In addition, it takes account of the context within which the personal data is being processed and our business practices.

2. Data Security

2.1. We will provide adequate data security in order to meet the principles of the GDPR. We have put the following safeguards in place to protect personal data which is processed by ecobirmingham:

a Each of our electronic databases has built-in IT security, backed up by copying to secure storage each night.

b External access to the databases is limited by passwords.

c Passwords are changed regularly and have to be complex (see Clause 2.5 of the Computers, Internet and Emails policy).

d Only staff who have to have access to databases for their work have the required logins and passwords to access such databases with two factor authentication.

e Although workstations automatically lock if left inactive for a specific period, users are advised always to lock their workstations when moving away from their desk. Data stored on a cloud-based network drive is automatically backed up.

f If logins and passwords are compromised then we will change these as soon as possible.

g Only users who need to access databases will have access to them.

h Other personal or special data may be held in local, small-scale documents, for example spreadsheets and word documents. These will be password protected and restricted to essential users on Sharepoint or BreatheHR.

i Personal or sensitive data should not be copied or downloaded to a lap-top

computer for local processing without the agreement of the Data Protection Officer and where it has been agreed that the data will be sufficiently protected and where this is necessary.

j Personal or sensitive data should not be stored on flash-drives or other external devices.

k Data taken out of the office, for example for home working or for a meeting, must always be done only with the prior agreement of the Data Protection Officer. If you have any concerns about data security of personal data taken offsite, please raise these with the Data Protection Officer.

l Hard copy data will be protected in locked filing cabinets. Only those who need to have access to the data will be given access to the key.

m Data is retained and disposed of according to need and to agreed retention periods. The overarching principle is that data should only be retained and stored for as long as such data has a legitimate purpose, and as specified in the Data Retention clause below and the Privacy Notice and after this they should be disposed of securely.

n At the end of the retention period, data should be disposed of and/or destroyed. Manual files should be shredded and disposed of in designated confidential waste sacks if appropriate. Electronic data should be deleted from central systems by the individual responsible for the data.

3. Data Retention

3.1 We will only retain personal data and sensitive data for as long as necessary for the purposes for which we collected it. After this time, it will be deleted or archived.

3.2 We will maintain retention policies and procedures to ensure personal data is deleted after an appropriate time unless a law requires that data to be kept for a minimum time.

3.3 We will make sure data subjects are provided with information about the period for which data is stored and how that period is determined in any applicable Privacy Notice.

3.4 Our business must ensure that personal data is securely disposed of when it is no longer needed. This will reduce the risk that it will become inaccurate, out of date or irrelevant.

3.5 The methods of disposal are to be appropriate to the nature and sensitivity of the documents concerned and include:

- Non-Confidential records: place in paper recycling bin

- Confidential records: shred documents and recycle or compost
- Deletion of Computer Records
- Transmission of records to an external body
- Cloud storage

Type of Record	Description	Retention Period
Financial and Legal Records	Deeds and Tax returns	12 years
Financial and Legal Records - Other	Budgets, Invoices, payments, accounting and audit reports, contracts, banking and compliance records, Trustee minutes	7 years
Marketing Records	Mailing lists and newsletter subscriptions	1 year after last action
Personnel Records	Emergency contacts and bank account details	After final salary payment or invoice has been paid
Personnel Records	Recruitment records, shortlisting, interviews, correspondence, personal details	1 year for unsuccessful candidates otherwise treat as a staff member below
Personnel Records – other	Payroll, employment contracts, contact details, appraisal and performance reviews, grievance and disciplinary and training records, Trustee details	6 years after last action
Administrative – Maintenance and Insurance	Maintenance contracts, Insurance documentation and claims records	10 years
Administrative – other	Risk assessments, accident and incident reports, PAT tests, Fire hazard tests, building reports, policies, constitution and governing docs.	Until superseded or 10 years
Fundraising	Applications, donor records, grant offer letters, grant terms, funding reports, correspondence, payment receipts	7 years
Projects	Partnership records, project	5 years

	feedback and survey data	
Emails	Email correspondence and attachments	Attachments should be filed on Sharepoint within 1 month or deleted. Relevant emails should be filed on sharepoint or hubspot, deleted or archived within 6 months.

4. Useful links and contacts

4.1. Our DPO at the time of publication of this Policy is Kam Bola. Our DPO can be contacted via kam@ecobirmingham.com. If our DPO is no longer the person detailed in this Policy, then you should contact a member of SMT for details of our current DPO.

4.2. The following internal policies are referred to in this Policy and contain additional information and guidance:

a *Privacy Notice and Cookies Policy*
b *Data Protection Policy – Staff*
c *Data Protection Policy – Volunteers and Trustees*
d *Social Media Policy*
e *Computers, Internet and Emails policy*

5. Administration of the Data Security Policy

5.1. If you have any queries or concerns about this Data Security and Retention Policy you should raise these with Michael Addison via michael@ecobirmingham.com.