Staff Data Security Protocol

1. Overview
	1. This policy should be read in conjunction with our Data Protection and Data Retention Policies. It defines:
* The role and responsibilities of the Data Protection Manager;
* The procedures in place for the safe and effective management of personal information relating to staff;
1. Data Protection Manager
	1. The Data Protection is responsible for:
2. Ensuring compliance with Data Protection Law;
3. Championing Data Protection within the organisation;
4. The design of data management systems and procedures;
5. Monitoring and enforcing compliance with these systems;
6. Ensuring the effective training of staff;
7. Coordinating and/or undertaking the tasks relating to the discharge of individual rights in relation to staff data (see clause 13 of our Data Protection Policy);
8. Ensuring appropriate technical and organisational measures to integrate data protection into the organisation’s activities;
9. Periodically reviewing the effectiveness of data security procedures.
10. Records Management
	1. The organisation collects staff personal data in the following ways:
11. Paper-based files and records;
12. Electronic records stored on our servers;
13. Electronic records stored on the cloud;
14. Emails, stored on our servers and online with a hosting organisation;
15. Cloud-based HR database;
16. Portable computers – laptops and tablets;
17. Company telephones;
18. Staff mobile telephones;
19. Tracker devices fitted to our vehicles;
20. CCTV.
	1. The organisation shares staff records with:
21. HMRC;
22. Our external payroll bureau;
23. Our auditors;
24. Pension and other benefit providers
25. Our retained HR advisers;
26. Our HR database hosts.
	1. These records are managed as follows:
27. Paper Files & Documents
	1. The following principles are to be observed:
	2. Invitations to external organisations or individuals to submit personal information by post (e.g. referees, job applicants) should request envelopes to be marked “Private & Confidential” and addressed to a named individual;
	3. “Private & Confidential” post should be opened only by the addressee, Data Protection Manager or [other individual];
	4. All documents should be stored within an appropriate paper file – for example, a file for each individual, for current staff, or a job vacancy file created to collect applicants for a job;
	5. Documents relating to special categories of personal data – otherwise known as sensitive personal data – should be removed from staff files and separately maintained in secure storage under the control of [title]. Access by others should be permitted only where necessary for specific pre-defined purposes as approved by the Data Protection Manager;
	6. Documents will be stored in a locked cabinet located [location];
	7. Access to staff data cabinets is restricted to [names], all of whom are keyholders;
	8. Files removed from and returned to storage must be recorded in a register kept for the purpose in the cabinet. The register records the files removed, identity of the remover; identity of the person receiving the files, date received, date returned;
	9. Files in relation to a particular staff member must not be accessed except by;
* Directors/Partners;
* The individual’s line manager or superior manager;
* HR officers;
* Finance officers for payroll purposes only;
* Others authorised on a case by case basis by Directors/Partners or the Data Protection Manager.
	1. Files removed from storage must be kept secure by the receiving individual and kept under lock and key except when in use;
	2. Files must not be removed from the premises except where an appropriate protocol is in place;
	3. Files and documents should be kept secure and not shared with unauthorised people;
	4. Documents should not be copied unless absolutely necessary. Copies should be kept secure in accordance with this protocol and securely destroyed where no longer required.
1. Electronic records stored on our servers
	1. The security of our network is managed by [job title] whose job description includes information security; OR
	2. The security of our network is managed by an independent IT contractor whose specification includes information security;
	3. Personal data is kept only in password-controlled folders/drives. The organisation of electric folders is structured to allow access to data only to the extent required for the role. For example, line managers can access only the data relating to their own team;
	4. Passwords must be changed regularly as recommended by the Data Protection Manager. Passwords must never be shared;
	5. Records relating to special categories of personal data are stored in secure folders/drives separately accessible only to [identities]. This data may be released only on their explicit authority of the Data Protection Manager;
	6. Computer users must log out of sensitive folders when away from their desks;
	7. In open plan or shared offices, you must take care to avoid information on screen being visible to unauthorised people;
	8. Electronically stored data must never be transferred or copied to servers other than those for which authorisation has been given by the Data Protection Manager.
2. Electronic records stored on the cloud
	1. The provisions of clause 5 above apply. In addition;
	2. The security of our cloud storage resources is managed by [job title] whose job description includes information security; OR
	3. The security of our cloud storage is managed by an independent IT contractor whose specification includes information security;
	4. Where data is transferred outside the European Union, an assessment of compliance with Chapter V of the GDPR is undertaken under the supervision of the Data Protection Manager. No data will be transferred until the appropriate safeguards have been put in place.
	5. Never share access to cloud stored data with anyone who has not been authorised;
3. Emails, stored on our servers and online with a hosting organisation
	1. Responsibility for email security resides with [job title];
	2. All emails which may contain personal data are encrypted. Encryption must not be de-activated under any circumstances;
	3. Care must be taken to ensure that personal data is transferred only to those who are appropriately authorised. Inadvertent data transfers can easily occur when copying-in further recipients or responding to group emails;
	4. Consideration should be given to data anonymisation and pseudonymisation where appropriate in order to mask the identities of data subjects.
4. Cloud-based HR database
	1. The organisation’s cloud HR database is provided by [BreatheHR/PeopleHR]. The Data Protection Manager ensures that an appropriate data processing contract is in place with the provider and that their security systems ensure GDPR compliance;
	2. [job title] is responsible for ensuring that access settings are aligned with the organisation’s data management protocol. This ensures that users have access only to personal data about others in the organisation where appropriate and necessary for their role.
	3. Users should carefully guard their passwords and never share them with anyone else, inside or outside the organisation;
	4. Uses should not take, print or distribute screenshots taken from the database except where absolutely necessary and where security can be assured.
5. Portable computers – laptops and tablets
	1. Portable computers must not be removed from the premises without appropriate authorisation from the Data Protection Manager;
	2. Where removed from our premises, portable computers must never, under any circumstances, be left unattended, even where locked in a vehicle;
	3. Loss of any device must be immediately reported to the Data Protection Manager;
	4. Portable computers should not be used in public spaces or where other unauthorised people may be able to see the screen;
	5. As with other computers, uses should always use password controlled access and log out when not using or away from the device;
	6. Loss of or unauthorised access to any device storing personal data must be reported immediately to the Data Protection Manager.
6. Company and personal mobile telephones
	1. Company provided mobile telephones may carry personal data in the form of contact information for other staff. This must be protected in the same way as other personal data;
	2. Similarly, staff may use their own phones for business use and collect contact details and other personal data. Personal phones may only be used where the provisions below are followed;
	3. Phones must use password controlled access;
	4. Data must not be transferred to other devices or storage without authorisation from the Data Protection Manager;
	5. Loss of or unauthorised access to any device storing personal data must be reported immediately to the Data Protection Manager.
	6. Staff leaving the organisation are required to erase personal data collected in relation to the organisation and will be required to sign a declaration to this effect;
7. Tracker devices fitted to our vehicles;
	1. Personal data is collected via our vehicle tracking system. The Data Protection Manager ensures that an appropriate data processing contract is in place with the provider and that their security systems ensure GDPR compliance;
	2. Tracker data downloaded and saved from the system is securely stored in password access controlled folders on our server;
	3. Access to personal data deriving from trackers is controlled by [the Data Protection Manager] who configures the permissions to ensure that only those necessarily requiring access may retrieve and view data.
8. CCTV
	1. The organisation uses CCTV in certain areas of the premises for various purposes. The use and management of personal data collected via CCTV is subject to our CCTV policy;
	2. Access to CCTV is controlled by the Data Protection Manager;
	3. Images collected via CCTV are stored on a rolling 28-day recording and are therefore automatically deleted after this period.
9. Shared Personal Data
	1. The organisation shares personal data with the categories identified in clause 3.2 above.
	2. The organisation has written contracts with data processors which include specifications for the processing authorised. These contracts are reviewed and approved by the Data Protection Manager.
	3. Staff interacting with external data processors must review the relevant contracts to ensure that only data covered by the processing contract is shared.
10. How should you process personal data for the Company?
	1. Everyone who works for, or on behalf of, the Company has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy and the Company’s Data Security and Data Retention policies.
	2. The Company’s Data Protection Officer/Data Protection Manager is responsible for reviewing this policy and updating the Board of Directors/Partners/Trustees on data protection responsibilities and any risks in relation to the processing of data. You should direct any questions in relation to this policy or data protection to this person.
	3. You should only access personal data covered by this policy if you need it for the work you do for, or on behalf of the Company and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.
	4. It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below). This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in your dismissal.
	5. [EMPLOYER TO ADD ANY OTHER RULES]
11. Training
	1. Training in the principles and practice of data security will be provided at induction and periodically thereafter as deemed necessary. All staff are required to undergo training and refusal may be treated as a disciplinary matter.