Hands On Payroll Giving
Data Retention Policy

1. Policy

1.1 It is the policy of Hands On Payroll Giving (HOPG) to ensure that data and documents are retained for the required amount of time as prescribed in law, and destroyed correctly once redundant. Even where information is not covered by the Act, the Data Protection Act principles suggest that information should be adequate, relevant, not excessive, accurate, up to date and not kept for longer than is necessary.

1.2 For data that is submitted to HOPG (electronic and hard-copy) for the purposes of individuals wishing to join Payroll Giving, HOPG will ensure that:

- data is held as required only so that an individuals' instructions can be acted upon.
- data is deleted with immediate effect if requested by the data subject whereby this will have no impact on legal responsibilities to keep data. If a request to receive data is received, HOPG will respond within 48 hours to confirm the action taken and any consequences as a result of this.
- if an instruction cannot be acted upon, data is classified as inactive and deleted at the time of monthly reconciliation.
- where held data is known to relate to an active donation, it is held until the donation is classified inactive and after which time data is deleted at the time of monthly reconciliation.
- where held data is not known to relation to an active donation, it is held for the purpose of providing a record of the financial transaction for seven years from the date of record, after which date data is classified as inactive and deleted at the time of monthly reconciliation.

1.3 For data that is held to allow HOPG to report to clients, all data must be kept in line with the relevant contractual agreement as signed by HOPG and the client. Should a working relationship end, any data provided by the client for reporting purposes will be deleted.

1.4 Information and documentation relating to HOPG business operations will be kept as detailed below:

Information / document type	Retention Period
Codes of Conduct and Practice	Indefinitely
Membership body policy and guidelines	Indefinitely
Insurance Certificates	40 years
Health and Safety Assessments	Indefinitely
Finance and salaries	7 years
Email archive (no personal data transferred by email)	7 years

AGM Minutes	Indefinitely
Contractual agreements	6 years after contract termination
Personnel records	7 years after employee leaves (reduced information required for references only)
Disciplinary records	2 years
Job application forms for unsuccessful candidates, interview notes, disclosures	1 year
Accident book	3 years after last entry

2. Deleting information

Electronic data and documents

Electronic data that is of a confidential nature is stored on a bespoke Data Management System (DMS). All data is classified and validated upon entry, data is not stored on endpoint devices. DMS is held encrypted with AES-CTR 256 cipher. All user activity is recorded via an audit which is accessible only at Director level. All records kept in systemized database; monthly database maintenance occurs with inactive data deleted.

DMS is hosted and the server environment maintained by Ridgeon Network (www.ridgeon-network.co.uk/), ISO27001 & ISO 9001 certified, based in Lutterworth, UK. No data is transferred outside of the EEA. All sensitive personal data is transferred only via SFTP and is deleted after download notification received. No sensitive personal data transferred via email.

Hard drives and PCs are disposed of by licensed secure computer disposal and WEEE waste services with certification provided and kept on file for seven years.

Hard copy documents

Any hard copy documents containing personal data are submitted to HOPG's office by tracked means. All data is entered into DMS and hard copies are shredded and disposed of securely. Any data captured hard copy is subject to HOPG's Information Security Policy terms.

3. Scope

This policy applies to all information HOPG collects, processes and stores in relation to business services to contracted charities and employers.

4. Responsibilities

4.1 All HOPG policies are covered in training and adhered to. Any misuse or inappropriate disposal of data is a breach of contract which will result in a disciplinary procedure.

4.2 All information users are responsible for reporting actual, suspected, threatened and potential information security incidents and for assisting with investigations as required, particularly if urgent action must be taken to prevent further damage.

4.3 Any incidents of inappropriate data use or disposal is to be reported to Penny Tapping-Forbes, Digital & Operations Director.