Information Management Policy

1. Policy Statement and Purpose

Information is a key resource required to deliver the Amaze charitable objects and to meet the expectations of our service users. Amaze is committed to creating, keeping and managing records which document its activities efficiently and systematically, to a standard appropriate to meet its purposes and the requirements of information legislation.

The aim of this policy is to provide a framework for managing information to enable Amaze to:

- deliver quality services by having timely access to meaningful and appropriate information
- make informed decisions
- be open and transparent
- protect vital records
- comply with the law
- work with partners
- protect our reputation and provide accountability over time

Maintaining appropriate and effective records management practices will help Amaze to deliver our services effectively and meet our statutory duties. By adopting this policy Amaze aims to ensure that our records, in whatever form they take, can be easily and efficiently located, accessed and retrieved, are better protected and securely stored, are disposed of safely and at the right time and that corporate risk is reduced through compliance with relevant legislation.

2. Scope

This policy applies to Amaze records held in all formats, whether paper, electronic or audio-visual, including e-mails produced or received in the conduct of business, and records held in business systems (i.e. Office 365, CharityLog, QuickBooks).

This policy applies to all Amaze employees (both permanent and temporary), also volunteers and Trustees if they hold any records on behalf of Amaze.

3. Roles and Responsibilities

The Chief Executive holds overall responsibility for setting strategic direction and ensuring that policies and processes are in place for the safe management of information.

The Management Team is responsible for producing and updating related policies and guidance and advising Amaze employees on their information and records management responsibilities.

All employees who receive, create, maintain or delete records are responsible for ensuring that they do so in accordance with the Amaze Information Management Policy and Amaze Data Protection & Confidentiality Policy. It is important that everyone recognises information as an asset and understands their information management responsibilities as set out in this policy.

4. Related policies and legislation

This policy should be read in conjunction with the Data Protection and Confidentiality Policy, IT policy and Business Continuity Plan.

Legislation relating to this policy includes:

- Data Protection Act 1998
- UK General Data Protection Regulation (UK GDPR)
- Freedom of Information Act 2000
- Lord Chancellor's Code of Practice on the Management of Records under Section 46 of the Freedom of Information Act 2000
- Charities Act 2011
- Companies Act 2006
- Taxes Management Act 1970
- Limitations Act 1980
- Employers' Liability (Compulsory Insurance) Regulations 1969
- Health and Safety At Work Act 1974
- Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013

5. Records Management

Records must be managed through their lifecycle: from creation, through storage and use, to disposal.

5.1 Creation and maintenance

All employees will:

- create, keep and manage records which document Amaze's principal activities.
- maintain records Amaze requires for business, regulatory, legal and accountability purposes. The requirements for different classes of records are documented in the Records Retention Schedule (Appendix 1).
- create records with meaningful titles so that they can be retrieved quickly and efficiently.
- make sure records are authentic, reliable, have integrity and remain usable. This includes making appropriate arrangements for ensuring the continuity and availability of information when employees leave, or during major organisational or technological change.

The Management Team will:

- ensure that appropriate storage arrangements are available for records in paper / hard copy
- ensure that appropriate back-up arrangements are in place for electronic records (including restoration of back-ups and disaster recovery if electronic records are damaged)
- ensure that business systems (i.e. Office 365, CharityLog, QuickBooks) are appropriately supported, maintained and protected by adequate security measures

5.2 Access to Records

- Records shall only be accessed by Staff for a business purpose.
- Service users can ask to access the records we hold about them under the UK GDPR.
- Records shall only be disseminated to the members of the public in line with the legislation framework currently in force and with any other relevant Amaze policy and procedure.
- For more details, refer particularly to the Amaze Data Protection and Confidentiality policy

5.3 Storage

Physical / paper records shall be kept in such a condition as to ensure continuing accessibility, intelligibility and usability throughout their whole life-cycle (including, for those selected for long-term or permanent retention, the period when they are kept in the archives).

Electronic records should only be retained in the Amaze Team Shared Folders accessible via Office 365. Records relating to Amaze business should not be retained on local computers, laptops, smartphone or other devices where they are not accessible to other staff, or available to the back-up system.

If working remotely on a computer, laptop, smartphone or other device not belonging to Amaze, all records can and should be accessed and stored via Office 365 portal. Because Office 365 does not currently allow for attaching documents to emails, it may be necessary to download a version of the file to a local computer, laptop, smartphone or other device for the purposes of attaching to an email and sending. In addition, any documents attached to CharityLog records need to be downloaded to be reviewed. When downloading information containing personal data, as soon as the attachment has been made and the email is sent, the file you should then be permanently deleted from the local PC or laptop (ie deleted and shredded) Free electronic shredding apps are available such as https://www.fileshredder.org/. Any files downloaded onto a local computer, laptop, smartphone or other device should be deleted and shredded when the staff member finishes work for the day. Staff failing to delete files will be in breach of Amaze's IT policy which may lead to disciplinary action.

E-mail correspondence also constitutes an element of electronic records, and therefore this guidance covers the disposal and retention of stored e-mails. Good practice dictates that all e-mails should be deleted after a maximum of three years, but if individual e-mails constitute formal records relating to any of the categories listed in Appendix1, the disposal and retention schedule should apply.

5.4 Disposal and retention

The Amaze Records Retention Schedule is available at Appendix 1. This should be routinely reviewed to comply with all relevant UK statutory provisions currently in force and must be modified as appropriate.

Records should be reviewed in accordance with the retention schedule when they are no longer required for on-going business or specific legal or regulatory purposes. At the end of their retention period arrangements should be made for secure destruction. Paper records

should be destroyed by using the confidential waste bags or by shredding the record using a cross cut shredder.

Electronic records should also be managed in accordance with the retention schedule. All new computer systems must include the functionality to delete or archive single records or groups of records at the end of their retention period. It is recommended that an intended disposal or review date is captured when creating electronic records.

All disposal and destruction should be approved by a member of the Management Team. Documentation of the disposal of records will be completed and retained.

Appendix 1: Records Retention Schedule

Record	Statutory minimum retention period	Source of statutory requirement (where known)	Recommended retention period
Governance			
Certificate of Incorporation and Certificates on Change of Name			Permanently
Memorandum and Articles of Association	Permanently		
Printed copies of resolutions submitted to Companies House	Permanently		
Annual returns	Permanently	Data Protection Act	
Trustee minutes and records of major agreements	Permanently	Data Protection Act	
Finance			
Payments records	6 years from the end of the financial year	Companies Act / Charities Act	
Invoice - revenue	6 years from the end of the financial year	Companies Act / Charities Act	
Petty cash records	6 years from the end of the financial year	Companies Act / Charities Act	
Bank records - cheques / paying-in counterfoils / statements	6 years from the end of the financial year	Companies Act / Charities Act	
Bank reconciliations	6 years from the end of the financial year	Companies Act / Charities Act	
Instructions to the bank			6 years after ceasing to be effective
Annual report and accounts (signed)	Permanently	Data Protection Act	
Interim report and accounts			Permanently
Budgets, forecasts and internal financial reports			5 years
Taxation records and tax returns, incl. P45 / P60 / P6	6 years plus current financial year	Taxes Management Act	

Annual return of taxable pay and tax deducted	6 years plus current financial year	Taxes Management Act	

Deeds of Covenant	6 years after last payment	Data Protection Act	
Legacies	6 years after the estate has been wound up	Data Protection Act	
Documents supporting entries in accounts for donations	3 to 6 years		
Contracts with suppliers, agents and others	6 years after expiry or termination of contract	Limitations Act	
Fixed Assets register	Permanently	Companies Act / Charities Act	
Rental and hire purchase agreements			*6 years after expiry*
Trust deeds and rules (pension schemes)	*Permanently*	*Companies Act / Pensions Act*	
Personal pension records, next of kin / expression of wishes forms	6 years after date of death	Data Protection Act	
Public liability policies	3 years after lapse	Data Protection Act	
Employers' liability policies	40 years	Employers' Liability (Compulsory Insurance) Regulations	
Other insurance policies			*Until claims under the policy are barred or 3 years after policy lapses, whichever is longer*
Health and Safety			
Health and Safety policy documents	Permanently	Health and Safety Act	
Accident books / accident records and reports	3 years after last entry or end of investigation if later	RIDDOR	
Assessment of risks under health and safety regulations, e.g. COSHH, asbestos	*Until revised*		

Staff and volunteer records*			
Job application and interview records	1 year	Limitations Act	
Personnel files and training records	6 years after employment ceases	Limitations Act	
Payroll and salary records, incl. overtime and expenses	6 years plus current year	Companies Act / Charities Act / Taxes Management Act	
Income tax records	6 years		
Annual return of taxable pay and tax paid	6 years		
Service user records:		Data Protection Act	
Compass data:	Records updated every 2-3 years when new Compass registration forms are completed. Then stored for another 3 years after the current registration period expires.		
Casework records:	Records held by Amaze about a parent carer, child or young person will be made inactive and anonymised by removing all personal data after 7 years of our last contact. We keep records for this period to facilitate ongoing support if the family returns to Amaze.		

*Exception for Staff and Volunteer Records:
Concerns about adults: If concerns have been raised about an adult's behaviour around children, the general rule is that you should keep the records in their personnel file either until they reach the age of 65 or for 10 years – whichever is longer (IRMS, 2016; Department for Education, 2018). This applies to volunteers and paid staff.