Data Retention Policy

Version	2
Policy code	POL-13
Author	Rise/HRH Flack
Approved by	FCA Steering Committee
Approval date	June 2023
Review date	June 2025

DATA RETENTION POLICY

1. Policy Statement

In the course of carrying out our various business activities, we collect information from a wide range of sources and generate a substantial volume of data that is retained as physical paper and/or electronic records. Appropriate retention of data is necessary for ouroperational performance and in some cases is required to fulfil statutory or other regulatoryand donor requirements or to evidence events and agreements in disputes.

However, the retention of data can lead to unnecessary and excessive use of electronic or physical storage space, and indefinite retention of personal data can breach the General Data Protection Regulation (2018). Failure to comply with the GDPR can lead to financial penalties from the Information Commissioner's Office of up to €20 million, or 4% annual global turnover – whichever is higher.

It is therefore essential that the FCA has appropriate systems and processes in place for the preservation and timely disposal of documents and records in line with business requirements and relevant legislation.

2. Purpose and scope for this policy

This policy sets out the FCAs approach to managing its information to ensure that records and documents are preserved in line with business and legislative requirements and that data is not retained for any longer than necessary. This policy applies to all parties of the FCA.

3. Who is covered by the Policy?

This policy specifically applies to all staff, volunteers, consultants, contractors, trustees and, as appropriate, partnership organisations, partner staff and third parties of the FCA and to all records that are created, handled, stored, or processed by the FCA,electronically (soft copy) or in paper (hard copy) form. All those people or groups to whom this policy applies should, as appropriate, be aware ofthis policy.

4. Who is responsible for this policy?

The Steering Committee have overall responsibility for the operation of this policy. They will ensure that adequate resources are available for the effective implementation of this Policy.

5. Data Storage

The rules on data storage vary according to the format of a data record, as set out below.

- **Electronic Records Storage - Documents, Email, Multimedia**

- All electronic documents, emails and multimedia records must be stored within the appropriate repository to ensure that applicable security, backup, retention and disposal controls can be applied.
- The individual who creates a record is responsible for ensuring that it is stored in the appropriate location. Statutory documentation listed in Appendix 2 must be stored in the relevant unit folder that has been provided centrally. Any files locatedoutside of this folder will be subject to the automated archiving rules, as per section 6.1.

- **Electronic Records Storage – Business Applications**
  All business application records must be stored within the relevant system (e.g. sponsor information must be stored on CARE). Data records may be extracted for analysis purposes and also stored temporarily in a secure location on the shared drive. Any extracted data must be erased from the shared drive after use.
- **Physical Records Storage**
  Physical records that are required for the day-to-day running of business operations must be stored when not in use in the designated cupboards, filing cabinets and pedestals (desk drawers). All storage units that contain personal and confidential data records must be locked at the end of the working day. All physical special category personal data records must be stored in an appropriate filing system when not in use and these must also always be locked at the end of the working day.

6. Data archiving

The rules on data archiving vary according to the format of a data record, as set out below.

6.1 Automated Electronic Records Archive - Documents, Email, Multimedia

Non-statutory electronic records stored on the shared or personal drives that have not been accessed for 2 years will be transferred to an electronic archive. Statutory records will be excluded from this process if they arestored in the designated departmental statutory records folder. Archived files maybe accessed in read-only format through the Archive drive until they are subsequently removed from the system, 7 years after their creation.

6.2 Physical Records Archive

Physical statutory records which are older than 2 years and don't need to be accessed on a day-to-day basis must be archived. The records will be archived either be being kept separately at Head Office (Avening park).

7. Data retention & disposal

The rules on data retention and disposal varies according to the format of a data record and the classification of the data contained within it (i.e. personal, special category personal or confidential data), as set out below.

7.1 Electronic Records Retention & Disposal - Documents, Email, Multimedia

The following retention rules apply to all FCA electronic documents, email and multimedia.

Non-Statutory Records - Schedules A-E:

Sch	Description	Status	Archive & Disposal Policy
A	Non-statutory shared & personal drive data	Live	Archive if **not accessed** for **2 years**
B	Archive data	Archive	Dispose of **7 years** after it was originally **created**

Sch	Description	Status	Archive & Disposal Policy
D	Email data (emailsonly)	Live	Mailbox items disposed of **2 years** after they were **created, sent or received.** All sent and received mailbox items also **logged and archived separately for 5 years**.
			Deleted Items folder contents automatically cleared after **30 days**
		Archive	Mailbox items disposed from the archive 5 years after they were sent or received
E	Multimedia data	Live	disposed of **3 years** after it was **created** (unless flagged otherwise by the Head of Comms)

Statutory Records - Schedules F & G:

Sch	Description	Status	Archive & Disposal Policy
F	Statutory Documents	Live	**Manually** disposed of by responsible unitin accordance with the retention rules in Appendix 2
G	Statutory Emails	Live	

The Head of unit (or role) specified against each record category in Appendix 2 is accountable for the manual disposal of records in line with the retention

rules (also listed in Appendix 2).

7.2 Electronic Records Retention & Disposal – Business Applications

The retention rules that apply to the FCA business application records are outlined in Appendix 2. The FCA will maintain a record of non-personalised aggregated data on past supporters in its CRM system to enable business planning and insight. To enable this, data on inactive or opted-out supporters is 'anonymised' at certain trigger points, such that they cannot be identified within the data set.

7.3 Physical Records Retention & Disposal Schedule

No physical record will be entered into either onsite or offsite archiving without a disposal date. The retention rules that apply to physical statutory documents are outlined in Appendix 2

8. Records backup schedule

Our data and our systems are automatically backed up to protect the FCA from the consequences of data loss, security breaches, system failure and disasters. Our electronic records are backed up and arestored in cloud systems.

9. Policy review

This Policy will be reviewed at least every two years. The next formal review will therefore take place in June 2025. This Policy may be reviewed earlier should there be a legislative or other significant need.

APPENDIX 1 – DEFINITION OF TERMS

Listed below are the definitions of certain terms as they are used in this policy.

Archive (electronic):	The FCAs read-only file repository that is used to store non-statutory shared and personal drive data that has not been accessed for 2 years, ahead of its disposal (5 years after creation).
Archive (physical):	The FCA's onsite archiving facility for physicaldocuments
Confidential data:	For this policy, any data that is not in the public domain and, if illegitimately accessed, altered, disclosed or destroyed could cause anon-negligible level of risk to the FCA, its staff, beneficiaries and/or supporters. Examples of confidential data include data protected by privacy legislation (i.e. personal data and special category personal data) and data protected by confidentiality agreements as well as internal-only documents and records, such as papers, reports, plans or emails etc.
Document:	Any physical or electronic report, article, spreadsheet, presentation,chart, plan, contract, drawing or similar.
Email:	For this policy, any item created in Microsoft Outlook or Gmail including emails, calendar items, contacts, tasks, notes and journal items.
IT User	Any individual (e.g. employee, volunteer, intern, apprentice, agency staff, consultant, contractor, trustee) working for or on behalf of the FCA who has access to the FCA corporate network and utilises any of our IT services to fulfil their role.
Multimedia:	Image, video and audio files or physical photographs or discs.
Non-statutory:	For this policy, any record that is retained by the FCA that is not required in order to comply with its legal, regulatory, compliance orcontractual obligations.

Personal data:	Data, whether facts or opinions, which relate to a living individual whocan be identified either from the data or from the data in combination with other information that is in the possession of, or likely to come into the possession of, the FCA.
Record:	For this policy, an organised collection of data items arranged for processing by a computer program or for consumption by an end user, either within a 'structured' database or 'structured' physical filing system or within 'unstructured' file repository, such as a document onthe shared or personal drives or a printed physical copy.
Special category personal data:	For this policy, information about an individual's characteristicsthat are protected under the GDPR (2018) and/or the Equality Act (2010), i.e. that relates to age, disability, health, sexual orientation, sex life, gender, gender reassignment, pregnancy and maternity, racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, health, criminal proceedings or convictions.
Statutory:	For this policy, any record that is retained by the FCA in order to comply with its legal, regulatory, compliance or contractual obligations.

APPENDIX 2 – STATUTORY RECORDS RETENTION & DISPOSAL SCHEDULE

Business Area	ID	Record	Disposal Policy	Accountable Head/Role
Corporate Governance	1	Records on establishment and development of the organisation'slegal framework and governance	6 years after end oflife of organisation	Corporate Governance
	2	Trustee Board papers and minutes	6 years after end oflife of organisation	Corporate Governance
	3	Management papers and minutes	6 years after end of financial year	Corporate Governance
	4	Subject Access Requests (requestsand responses)	6 years fromresponse	Corporate Governance
	5	Litigation with third parties	6 years after settlement of case	Corporate Governance
	6	Provision of legal advice	6 years from date of advice	Corporate Governance
	7	Audit reports	6 years from completion	Corporate Governance
	8	Fraud Investigations	6 years from completion or 5 years after award completion (whichever is later)	Corporate Governance
	9	Strategic plan, business plan, riskplans	6 years from completion	Corporate Governance
Data Protection	10	Consent (where unstructured data)	6 years after consent expired	Data processing unit
	11	Privacy notices and index	6 years after end oflife of organisation	Data processing unit
	12	Record of Processing Activities	6 years after end oflife of organisation	DPO

	13	Subject Access Requests	6 years after end oflife of organisation	DPO
	14	Subject Access Request case data	90 days after the SAR case is closed	DPO

Business Area	ID	Record	Disposal Policy	Accountable Head/Role
Financial Management	15	Financial records	6 years after date of signing of accounts or, as applicable, 5 years after award completion (whichever is later)	Finance
	16	Property acquisition (purchase, donation, rental, transfer) Deeds andcertificates	6 years after end of ownership/asset liability period	Finance
	17	Property leases	15 years after expiry	Finance
	18	General contracts and agreements	6 years after contract termination	Authorising Unit
	19	Unsuccessful tender documents	1 year after tender awarded	Authorising Unit
Award Management	20	Unsuccessful application	2 years after decision	Authorising Unit
	21	Successful award file	6 years afterend of award	Authorising Unit
	22	Job applications and interview records for unsuccessful applicants	6 months after interview	HR
	23	Payroll records – salaries and otherpayments through payroll	6 years	HR

Human Resource Management	24	Payroll records - Maternity, Paternity, Adoption and SSP records	3 years after endof the tax year	HR
	25	Pension details - name, National Insurance number, opt-in notice and joining notice. (Kept by Standard Life)	6 years after effective date	HR
	26	Pension details – opt-out (kept byStandard Life)	4 years after optout	HR
	27	A summary of record of service e.g. name, position, dates ofemployment, pay	6 years after end of employment	HR
	28	Timesheets, pay records and supporting documents such as contracts and contractual letters for employees charged to awards	5 years after payment of awardbalance	HR

Business Area	ID	Record	Disposal Policy	Accountable Head/Role
	28	Evidence of right to work	2 years after end ofemployment	HR
	29	All other HR documents	1 year after end of employment	HR
Supporter	30	Individual Giving supporter financial and banking data (excluding paymentcard details)	12 months after end of regular gift	Individual Giving
	31	Gift Aid authorisation	6 years after end of regular gift	Individual Giving
	32	Payment card data	Immediately after transaction	Individual Giving

Stewardship	33	Prospects (e.g. as considered by Major Partnerships and CEO Office)who have not been successfully converted into active supporters	3 years after become inactive	MPU
	34	Inactive but not opted-out supporters'personal data (e.g. contact details, preferences and history etc.) for correspondence and marketing purposes. This also refers to Individual Giving Prospects	3 years after become inactive	Individual Giving
Safeguarding	35	Child welfare concerns referred to alocal authority	6 years after referral	Child SafeguardingFocal Point
	36	Child welfare concerns not referred toa local authority	1 year after child ceases to be associated with FCA	Child SafeguardingFocal Point
	37	Concerns about an adult relating tochild safeguarding	10 years	Child SafeguardingFocal Point
	38	DBS check outcome	1 year after end of relationship with FCA	Child SafeguardingFocal Point