Plan International UK
DATA RETENTION POLICY

DOCUMENT CONTROL INFORMATION:

Title:	Data Retention Policy
Author (Responsible):	Head of IT
Owner (Accountable):	Chief Operating Officer
Directorate:	Operations
Contact:	Head of IT
Version no:	2.1
Status:	Final
Reviewed by (Consulted):	Management Board, Head of Corporate Governance, Head of Finance, Head of HR, Head of Individual Giving, Property & Facilities Manager, IT Operations Manager
Approved by:	Management Board
Date of approval:	9 April 2019
Applicable to (Informed):	All IT users
Issued on:	12 April 2019
Related policies & procedures:	Data Protection Policy, Unstructured Personal Data Standard, Code of Conduct, Information Security Policy, Business System Data Disposal Process

DECISION-MAKING:

Decision	Accountable	Responsible	Consulted	Informed
All matters regarding this policy	COO	Head of IT	Management Board, Head of Corporate Governance, Head of Finance, Head of HR, Head of Individual Giving, Property & Facilities Manager, IT Operations Manager	All employees and others

Contents

Appendices

1.0 INTRODUCTION

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 our operational performance and in some cases is required to fulfil statutory or other regulatory and 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 Plan International UK 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.

2.0 PURPOSE

This policy sets out Plan UK's 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.

3.0 SCOPE

This Data Retention Policy is a subcomponent of the Information Security Policy. This policy specifically applies to:

- all staff, volunteers, consultants, contractors, trustees and, as appropriate, partnership organisations, partner staff and third parties of Plan UK.
- all records that are created, handled, stored, or processed by Plan UK, electronically (soft copy) or in paper (hard copy) form.

All those people or groups to whom this policy applies should, as appropriate, be aware of this policy.

4.0 DATA STORAGE

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

4.1 Electronic Records Storage - Documents, Email, Multimedia

All electronic documents, emails and multimedia records must be stored within the appropriate repository (shown below) to ensure that applicable security, backup, retention and disposal controls can be applied. Note that the letters listed in the

table below (A – G) relate to the corresponding retention and disposal schedule that is outlined in section 6.1. Here, “prohibited” means that it must not be done, even though the drives will in fact allow you to store data in them.

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 located outside of this folder will be subject to the automated archiving rules outlined in section 5.1.

Record Type	Category	Shared Drive (S:\)	Archive (R:\)	Personal Drive (P:\)	Media Drive (U:\)	Scratch Area (X:\)	Email System
Document	Non-Statutory	A	B	A	Prohibited	C	D
	Statutory	F	Prohibited	F	Prohibited	Prohibited	Prohibited
Multimedia	Non-Statutory	A	Prohibited	A	E	C	D
Email	Non-Statutory	A	B	A	Prohibited	Prohibited	D
	Statutory	G	Prohibited	G	Prohibited	Prohibited	Prohibited

4.2 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 (S:\) drive. Any extracted data must be erased from the shared drive after use.

4.3 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) that have been provided by Property & Facilities Management. 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.

5.0 DATA ARCHIVING

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

5.1 Automated Electronic Records Archive - Documents, Email, Multimedia

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

5.2 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 the Finsgate building or offsite using the document archiving service provided by Property & Facilities Management. Offsite records can be recalled within 24 hours by request to Property & Facilities Management.

6.0 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.

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

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

Non-Statutory Records - Schedules A-E:

Sch.	Description	Status	Archive & Disposal Policy
A	Non-statutory shared (S:\) & personal (P:\) drive data	Live	Automatically archived if **not accessed** for **2 years**
B	Archive (R:\) data	Archive	Automatically disposed of **7 years** after it was originally **created**
C	Scratch Area data	Live	Automatically disposed of if **not accessed** for **30 days**

Sch.	Description	Status	Archive & Disposal Policy
D	Email data (emails only)	Live	Mailbox items automatically 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 automatically disposed from the archive 5 years after they were sent or received
E	Multimedia data	Live	Automatically disposed of **3 years** after it was **created** (unless flagged otherwise by the Head of Comms or Head of Individual Giving)

Statutory Records - Schedules F & G:

Sch.	Description	Status	Archive & Disposal Policy
F	Statutory Documents	Live	**Manually** disposed of by responsible unit in 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).

6.2 Electronic Records Retention & Disposal – Business Applications

The retention rules that apply to Plan UK business application records are outlined in Appendix 2. Plan UK 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 dataset.

6.3 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.

7.0 ELECTRONIC RECORDS BACKUP SCHEDULE

We back up our data and our systems to protect Plan UK from the consequences of data loss, security breaches, system failure and disasters. Our electronic records are backed up by the IT department in accordance with the Backup Schedule outlined below and are stored remotely as per the IT Service Continuity Plan.

Electronic Data Backup Schedule:

Records by Location	Backup Frequency	Daily Backups	Monthly Backups (taken on last day of month)
Shared drive (S:\) records	Daily	Dispose after 1 month	Dispose after 2 years
Personal drive (P:\) records	Daily	Dispose after 1 month	Dispose after 2 years
Scratch area drive (X:\) records	Never	Not backed up	
Multimedia drive records (U:\)	Daily	Dispose after 1 day	N/A
Legacy email system records [NB to remove category once no longer applicable]	Daily	Dispose after 1 month	Dispose after 1 year
Archived electronic records	Monthly	None	Dispose after 1 year since creation
Business application records	Daily	Dispose after 1 month	Dispose after 2 years

APPENDIX 1 - DEFINITION OF TERMS

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

Archive (electronic):	Plan UK's read-only file repository that is used to store non-statutory shared (S:\) and personal (P:\) drive data that has not been accessed for 2 years, ahead of its disposal (5 years after creation).
Archive (physical):	Plan UK's onsite at Finsgate and offsite archiving facility for physical documents that is made available by Property & Facilities Management.
Confidential data:	For this policy, any data that is not in the public domain and, if illegitimately accessed, altered, disclosed or destroyed could cause a non-negligible level of risk to Plan UK, 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, 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 Plan International UK who has access to the Plan International UK corporate network and utilises any of our IT services to fulfil their role.
Multimedia:	Image, video and audio files or physical photographs, cassettes or discs.
Non-statutory:	For this policy, any record that is retained by Plan UK that is not required in order to comply with its legal, regulatory, compliance or contractual obligations.
Personal data:	Data, whether facts or opinions, which relate to a living individual who can 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, Plan UK.

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 on the shared (S:\) or personal (P:\) drives or a printed physical copy.
Special category personal data:	For this policy, information about an individual's characteristics that 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 Plan UK in order to comply with its legal, regulatory, compliance or contractual obligations.
Scratch area:	An alternative electronic data storage area to the shared (S:\) drive that is designed for easily sharing and collaborating on documents and multimedia such as photos and videos at low cost. The scratch area is accessible through Windows Explorer on the X:\ drive and is open to all IT users. There are no internal security controls in place, which means that all IT users may access all files stored in the scratch area, and therefore, it must never be used to store confidential data. Data stored in the scratch area is not backed up (and is therefore not recoverable in the event of loss) and all data stored there is automatically deleted 30 days after it was last accessed.

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's legal framework and governance	6 years after end of life of organisation	Corporate Governance
	2	Trustee Board papers and minutes	6 years after end of life of organisation	Corporate Governance
	3	Management papers and minutes	6 years after end of financial year	Corporate Governance
	4	Subject Access Requests (requests and responses)	6 years from response	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, risk plans	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 of life of organisation	Data processing unit
	12	Record of Processing Activities	6 years after end of life of organisation	DPO
	13	Subject Access Requests	6 years after end of life 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 and certificates	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 after end of award	Authorising Unit
Human Resource Management	22	Job applications and interview records for unsuccessful applicants	6 months after interview	HR
	23	Payroll records – salaries and other payments through payroll	6 years	HR
	24	Payroll records - Maternity, Paternity, Adoption and SSP records	3 years after end of 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 by Standard Life)	4 years after opt out	HR
	27	A summary of record of service e.g. name, position, dates of employment, 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 award balance	HR

Business Area	ID	Record	Disposal Policy	Accountable Head/Role
	28	Evidence of right to work	2 years after end of employment	HR
	29	All other HR documents	1 year after end of employment	HR
Supporter Stewardship	30	Individual Giving supporter financial and banking data (excluding payment card 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
	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 a local authority	6 years after referral	Child Safeguarding Focal Point
	36	Child welfare concerns not referred to a local authority	1 year after child ceases to be associated with Plan	Child Safeguarding Focal Point
	37	Concerns about an adult relating to child safeguarding	10 years	Child Safeguarding Focal Point
	38	DBS check outcome	1 year after end of relationship with Plan UK	Child Safeguarding Focal Point

For any other type of record, or if you have any questions, please liaise with your Head of Unit in the first instance and then, as necessary, with either the Head of IT or the Head of Corporate Governance.