



ANGLING TRUST

Angling Trust

PD69 AT Data Retention Policy

DOCUMENT CONTROL	
Version Number	1.0
Document Author	Alistair Middleton
Lead Director	Simon Bourne
Review Frequency	Biennial
Next Review Date	TBC
Purpose	<p>To ensure everyone involved with records management in the Trust is aware of their responsibilities and roles regarding agreed retention periods, and to ensure records are retained, rationalised or deleted in line with the appropriate standards:</p> <ul style="list-style-type: none"> • Legal • National guidelines (e.g. Finance and HR) • Internal limits based on best practice and alignment to similar membership organisations.

REVISION HISTORY			
Version	Date	Summary of Changes	Author
1.0	August 2021	New Procedure	Alistair Middleton
1.2	Nov 2021	Updated format to include front sheet and Doc Control Sheet	Sue Woollard
1.3	Dec 2021	Further revision to include reference to HR files and FL practises	Stuart Sharp
1.4	Jan 2022	Proofread for spelling and grammar errors	Georgia Neal

Approvals		
Approved by: ATB/FLC/CEO/COO/GOV COMM	Date	Version

Distribution				
Audience	Method	By whom	Date of issue	Version
Staff, Directors, Volunteers				

Contents

Purpose of this Policy	4
What is Retention?	4
Creation of this Policy	5
When archiving, rationalising or deleting information	8
Training and other useful source reading	8
Fish Legal	8
Appendix 1 – Retention Periods in Chronological Order	8

Purpose of this Policy

- Everyone involved with receiving, storing and transmitting data should be aware of their role and responsibilities.
- Everyone involved should have the guidance to understand what types of data they or their team holds and what retention periods are instructed by the Trust. E.g. minimum/maximum period or perpetually held.
- Everyone involved should have the power to archive, rationalise and delete paper records/ electronic data in line with the type of record and the set retention period stated in the policy.
- Team managers have duties to oversee that records are not being kept beyond their stated periods to avoid facilitating GDPR issues or increasing the likelihood of the risk of a serious data breach. Likewise, to ensure data is not deleted whilst it is still needed or required to be retained under law or other unique reasons.

What is Retention?

The continued possession, use or control of information.

Scope

- Paper records (invoices, receipts, letters, correspondence, lists)
- Electronic records
- Other electronic or physical media

Examples

- Physical paper record information kept on Trust premises, 3rd party storage facilities or within the home of staff whilst performing remote duties.
- Electronic records held in core business systems – e.g CRM, website, finance applications and HR systems.
- Data held within Trust devices or specified storage systems, e.g Onedrive, Sharepoint, CCloud
- Paper records kept in drawers or in lever-arch files (invoices, receipts, letters, correspondence, lists etc)
- Photographs and associated content - e.g. left on devices or held on Trust data storage systems

Creation of this Policy

Research and consultation was conducted using the below sources:-

- “National guidance and legal limits for corporate and legal records” (including ICO parameters)
- “Records Management Society of Great Britain” guidelines
- Research into limits agreed and published by membership organisations similar to ourselves
- Some local Trust decisions in terms of best practice
- [Guide to Email Retention and UK Compliance Laws](#)
- [Board Minute Legislation Guidance](#)
- [HR Record Keeping](#)

Other References

- Data Protection Act 2018
- Companies Act 2006
- General Data Protection Regulation (GDPR)

Review of this policy

Review is essential as standards may change. The internal effectiveness of any rationalisation of Trust records in line with this retention policy can be potentially analysed leading to further changes or adjustments to retention periods.

Outcomes

It is paramount to drive decisions around the deletion and removal of data to reduce the risk of data breach and leakage. It is also a key measure to avoid pressure on storage space, both internally and with 3rd parties.

Data	Retention Period or action
Incorrect data on current members and coaches	Any out-of-date material should be deleted immediately i.e. as soon as an address is updated, or an emergency contact is updated for example
Current members and coaches (including Orgs)	Retention period is ‘for the start date of the membership whilst valid in terms of payment to the trust’. Once this membership is ended (i.e. cancellation by the individual) then the member is instantly (by the CRM) identified as ‘Lapsed’ (see below). If they re-join at any point their original membership number is reassigned by the system and the retention period starts from day 1 again.
Lapsed members and coaches	5 years. Note this is consecutive years of being in a lapsed/expired state.
Incomplete members (user not completing a successful membership or payment via website).	These are picked up by the E-connect system triggering an email and follow up phone calls to attempt a conversion into a valid membership. Any that remain ‘incomplete’ are kept in this ‘type field’ in the CRM. The supplier is informed every 6 months to clear this history. Therefore, 6 months is in effect the retention period of ‘incompletes’.

Data on prospective members (marketing)	Kept for 3 years from initial contact date if they do not become a member.
Prize draw, auction and raffle data	3 years – any ‘pass’ of information to marketing can only be filtered by users that ‘opted in’ on the web form.
Subscriber lists (AT newsletter and Get Fishing)	When live members update any out of date information (i.e. new email address) the previous information should be deleted. Lapsed members and other users that have subscribed to the AT or similar newsletters that have not opened an email for 6 months (stats via E-Connect) should be deleted. Any invalid email address returns from the E-Connect system should be permanently deleted.
Data on volunteer contact details	Claims for personal injury can be brought up to three years later and any case might need to access a record of training or equipment provided etc. Therefore, a 3-year retention for all volunteer records
Forum, event data	3 years Note: any ‘pass’ of PID information to marketing team can only be filtered by users that ‘opted in’ to AT marketing.
Campaigns	3 years from initial contact, however anyone who has not opened an email in direct connection to the said campaign for 6 months is deemed no longer directly supportive and should be removed.
Match Competition data	5 years. Note: data beyond this is not completely removed as ‘results’ have historical value. Therefore, results should be kept indefinitely, but information at levels ‘lower’ than result tables should be removed after 5 years.
Donations / Legacy	In line with financial data (6 years).
Emails (in Outlook and stored outside of this on other platforms)	Emails could cover a broad range of topics and interactions i.e. emails between work colleagues on small matters/emails between Board Members on a high-level business matter. There is a comprehensive booklet from Barracuda below to explain this: https://www.cybersecuritymart.com/wp-content/uploads/2017/03/Barracuda-ArchiveOne-WP-Guide-to-Email-Retention-and-UK-Compliance-Laws-UK.pdf In practice this means each AT member of staff should deploy their judgement of 12 months for basic housekeeping up to important business emails for 6 years since sent or received. Obviously, in terms of ‘policy’ this is down to judgement of each individual with support and advice from Senior Management, the Trust DPO and the Trust Governance Manager.
Employee Personnel records (HR) and other organisational employee records.	We collect data relating to our employees (HR records) – including information on pay, sickness absence, hours worked etc. With HR records there are, firstly, legal checklists providing statutory retention periods in relation to the Data Protection Act 2018., and, secondly, the General Data Protection Regulation (GDPR) which gives recommendations for keeping some related information. Mandatory retention periods <ul style="list-style-type: none"> • Accident books/reports – 3 years from the date of last entry • First aid, fire warden training – 6 years after employment • Health and Safety training – 5 years after employment

	<ul style="list-style-type: none"> Working time documents including overtime, annual holiday, jury service etc. 2 years after they were made. <p>Recommended (non-statutory) retention periods</p> <p>e.g. personnel records, recruitment applications, right to work in UK, SSP records etc.</p> <p>This also covers senior executive records and all records within this regarding applications and any member voting on such matters.</p> <p>For many types of HR records there is no definitive retention period; it is up to AT to decide how long to keep them (based on type of record). For example: some HR managers keep employee records until they reach the age of 100 for pension purposes. Also, contractual claims and defamation claims rely on data being available (i.e. going back to references or interview notes).</p> <p>In the absence of statutory mandatory retention periods, Angling Trust will adopt the following retention periods:</p> <ul style="list-style-type: none"> Job applications from unsuccessful candidates will be retained for 6 months from the later of closing date or appointment of the successful candidate. Personnel files for employees will be retained for 6 years after employment has ceased. <p>Further guidance / suggested retention periods for such can be found here: -</p> <p>https://www.cipd.co.uk/knowledge/fundamentals/people/hr/keeping-records-factsheet#gref</p>
<p>Finance / Payroll & other corporate information</p>	<p>Mandatory retention periods</p> <ul style="list-style-type: none"> Accounting records - 6 years – Section 388 Companies Act 2006 Records of COVID-19 related record keeping (furlough) 6 years Income tax, NI returns and correspondence with the HMRC – not less than 3 years after the end of the financial year to which they relate. Salary records – 6 years from the end of the tax year they relate to. VAT deferral (Covid 19) – 6 years <p>Recommended (non-statutory) retention periods can be found below – this includes Companies House information and Trust deeds and rules.</p> <p>https://www.cipd.co.uk/knowledge/fundamentals/people/hr/keeping-records-factsheet#gref</p>
<p>Subject Access Requests</p>	<p>1 year following completion of the request (Data Protection Act 2018)</p>
<p>Data Breach and incident log records to ICO</p>	<p>5 years after incident submitted</p>
<p>Board / ARAC / committee minutes, agenda and papers.</p>	<p>At least 10 years – legal requirement under the Companies Act 2006 - but could be considered for keeping permanently as a historical record.</p> <p>Guidance can be found here: -</p>

	https://www.legislation.gov.uk/ukpga/2006/46/part/10/chapter/9/crossheading/records-of-meetings-of-directors#:~:text=248Minutes%20of%20directors'%20meetings,the%20date%20of%20the%20meeting.
--	---

***Please see Appendix 1 for a version of this table in chronological order**

When archiving, rationalising or deleting information

- Consult with your team manager or appropriate senior team manager
- Further advice / steer should be available from the Trust Governance Manager or DPO role.
- Make a note of such events within your team documentation e.g. why has information been removed and under what criteria and permission.

Training and other useful source reading

Staff should always be encouraged to be aware of key Trust policies, in particular data protection and any mandatory data protection training assigned to staff in the online training portal.

Annual Review

Managers and/or individuals must conduct an annual review of documents under their control. This should be kept in the relevant team's SharePoint area.

Information on Personal Devices

AT information should not be kept on personal devices (i.e. local drive/desktop) where AT devices have been issued. If there is an express need to keep information on a personal device, care should be taken to ensure extra levels of protection such as using a unique password to protect the information. This information must be deleted immediately upon termination of employment/service.

AT Directors

Upon termination of services, Directors/Committee members are required to remove all AT material in any format that is held on all personal devices they have used during the period of their directorship. This is to include AT business emails sent to their personal email account.

Exceptions

Where a case has been brought against the Angling Trust, any and all records pertaining to that case will immediately become exempt from the above retention periods and must be retained for as long as the case requires their use.

Fish Legal

Fish Legal has its own retention policy around their illegal advice and case work. For all HR and other business purposes, Fish Legal adopts the same retention policies as Angling Trust. Please refer to document PD24 – FL Case and Advice Work File Retention Policy which is available in the Staff Information Area of SharePoint. Appendix 1 – Retention Periods in Chronological Order

Appendix 1 – Retention Periods in Chronological Order

Retention Period	Data	Action
Immediately	Incorrect data on current members and coaches	Any out-of-date material should be deleted immediately i.e. as soon as an address is updated, or an emergency contact is updated for example
	Subscriber lists - invalid email address returns	These can be found on the E-Connect system. They should be deleted permanently.
	Subscriber lists - old data from live members after they update their information e.g. an old email address	These should be deleted permanently.
6 months	Incomplete members (user not completing a successful membership or payment via website)	These are picked up by the E-connect system triggering an email and follow up phone calls to attempt a conversion into a valid membership. Any that remain 'incomplete' are kept in this 'type field' in the CRM. The supplier is informed every 6 months to clear this history. Therefore, 6 months is in effect the retention period of 'incompletes'.
	Job applications from unsuccessful candidates	In the absence of statutory mandatory retention periods, Angling Trust will retain such data for 6 months from the later of closing date or appointment of the successful candidate.
	Subscriber lists - lapsed members and other users that have subscribed to the AT or similar newsletters that have not opened an email for 6 months	These stats can be found via E-Connect.
12 months	Emails (in Outlook and stored outside of this on other platforms) deemed basic housekeeping.	<p>12 months since sent/received</p> <p>Emails could cover a broad range of topics and interactions i.e., emails between work colleagues on small matters/emails between Board Members on a high-level business matter. There is a comprehensive booklet from Barracuda below to explain this: Guide to Email Retention and UK Compliance Laws</p> <p>Each AT member of staff should deploy their judgment with support and advice from senior management, the Trust DPO and the Trust Governance manager.</p>
	Subject Access Requests	1 year following completion of the request (Data Protection Act 2018).

2 years	Working time documents including overtime, annual holiday, jury service etc.	These fall under the legal retention periods stated in the Data Protection Act 2018. They should be retained for 2 years after they were made.
3 years	Accident books/reports	These fall under the legal retention periods stated in the Data Protection Act 2018. They should be retained for 3 years from the date of last entry.
	Date on prospective members (marketing)	Kept for 3 years from initial contact date if they do not become a member.
	Prize draw, auction and raffle data	Kept for 3 years. Kept for 3 years from initial contact date if they do not become a member.
	Data on volunteer contact details	Claims for personal injury can be brought up to three years later and any case might need to access a record of training or equipment provided etc. Therefore, a 3-year retention for all volunteer records.
	Forum, event data	3 years. Note: any 'pass' of PID information to marketing team can only be filtered by users that 'opted in' to AT marketing.
	Campaigns	3 years from initial contact, however anyone who has not opened an email in direct connection to the said campaign for 6 months is deemed no longer directly supportive and should be removed.
	Income tax, NI returns and correspondence with HMRC	Not less than 3 years after the end of the financial year to which they relate.
5 years	Lapsed members and oraches (including organisations)	5 consecutive years of being in a lapsed/expired state.
	Match Competition data	5 years. Note: data beyond this is not completely removed as 'results' have historical value. Therefore, results should be kept indefinitely, but information at levels 'lower' than result tables should be removed after 5 years.
	Health and Safety training	These fall under the legal retention periods stated in the Data Protection Act 2018. These should be retained for 5 years after employment.
	Data breach and incident log records to ICO	5 years after incident submitted.
6 years	First aid, fire warden training	These fall under the legal retention periods stated in the Data Protection Act 2018.

		These should be retained for 6 years after employment.
	Personnel files for employees	6 years after employment has ceased
	Accounting records	6 years per Section 388(4)(b) of the Companies Act 2006
	Records of COVID-19 related record keeping (furlough)	6 years
	Salary records	6 years from the end of the tax year they relate to
	VAT deferral (COVID-19)	6 years
	Emails (in Outlook and stored outside of this on other platforms) deemed important business information	<p>6 years since sent/received.</p> <p>Emails could cover a broad range of topics and interactions i.e., emails between work colleagues on small matters/emails between Board Members on a high-level business matter. There is a comprehensive booklet from Barracuda below to explain this: Guide to Email Retention and UK Compliance Laws</p> <p>Each AT member of staff should deploy their judgment with support and advice from senior management, the Trust DPO and the Trust Governance manager.</p>
	Donations / Legacy	In line with financial data, it should be kept for 6 years.
10 years	Board / ARAC / Committee minutes, agenda and papers	<p>At least ten years – legal requirement under the Companies Act 2006 - but could be considered for keeping permanently as a historical record.</p> <p>Guidance can be found here: Board Minute Legislation Guidance</p>
Exercise your own judgment	Current members and coaches (including Orgs)	<p>Retention period is ‘for the start date of the membership whilst valid in terms of payment to the trust’. Once this membership is ended (i.e. cancellation by the individual) then the member is instantly (by the CRM) identified as ‘Lapsed’ (see below).</p> <p>If they re-join at any point their original membership number is reassigned by the system and the retention period starts from day 1 again.</p>
	Other HR records	For many types of HR records there is no definitive retention period; it is up to AT to decide how long to keep them (based on type of record). For example: some HR managers keep employee records until they reach the age of 100 for pension purposes. Also, contractual

		<p>claims and defamation claims rely on data being available (i.e. going back to references or interview notes).</p> <p>Further guidance / suggested retention periods for such can be found here:</p> <p>HR Record Keeping</p>
	<p>Other Emails</p>	<p>Emails could cover a broad range of topics and interactions i.e. emails between work colleagues on small matters/emails between Board Members on a high-level business matter. There is a comprehensive booklet from Barracuda below to explain this:</p> <p>Email Retention Guide and UK Compliance Laws</p> <p>In practice this means each AT member of staff should deploy their judgement of 12 months for basic housekeeping up to important business emails for 6 years since sent or received. Obviously, in terms of 'policy' this is down to judgement of each individual with support and advice from Senior Management, the Trust DPO and the Trust Governance Manager.</p>